Tesis TSP Gutierrez Mateo Margiori

por Margiori Janiz GUTIERREZ MATEO

Fecha de entrega: 20-nov-2021 03:53p.m. (UTC-0500)
Identificador de la entrega: 1708671210
Nombre del archivo: Tesis_TSP_de_Gutierrez_Mateo_Margiori.docx (1.39M)
Total de palabras: 17777
Total de caracteres: 97633

FACULTAD DE INGENIERIA

Carrera de Ingenieria Empresarial y de Sistemas

APLICACIÓN DE METODOLOGÍA DE RIESGO OPERACIONAL PARA MEJORAR EL PROCESO DE GESTIÓN DE TECNOLOGIA EN UNA ENTIDAD FINANCIERA

Trabajo de Suficiencia Profesional para optar el Título Profesional de Ingeniero Empresarial y de Sistemas

MARGIORI JANIZ GUTIERREZ MATEO
(0000-0002-6245-7407)

Asesor:
Mg. Carlos Antonio Flores Bashi
(0000-0002-9304-885X)

Lima – Perú

2021

Índice

Índice de Figuras

Índice de Tablas

Introducción

El presente trabajo de suficiencia profesional tiene como propósito la mejora del proceso de gestión de tecnología a partir de la aplicación de las metodologías de la gestión de riesgo operacional en una entidad financiera peruana, la cual es liderada por la Caja de Pensiones Militar Policial que inició sus operaciones en el año 2004 con la autorización de la Superintendencia de Banca y Seguros del Perú.

En la actualidad, los bancos tradicionales se enfrentan a un mercado cada vez más competitivo, por lo cual el sector financiero está presentando cambios debido a la transformación digital. Así mismo, esto ha dado lugar a nuevos modelos de negocios y servicios donde los consumidores exigen mayor inmediatez, experiencia y seguridad en los servicios y canales digitales para la operatividad diaria. Por ello, es necesario la evaluación de los procesos bajo un enfoque de riesgos para así garantizar la estabilidad financiera y evitar pérdidas operacionales, teniendo en cuenta que el sector financiero debe cumplir con un marco regulatorio.

El presente trabajo de suficiencia profesional comprende de cinco capítulos:

Capítulo 1: Comprende las generalidades de la empresa, tales como datos, ubicación, giro, tamaño, reseña, organigrama, visión, misión, productos y relación con la sociedad.

Capítulo 2: Comprende el planteamiento del problemas, contextualización, formulación, objetivos, justificación, alcances y limitaciones.

Capítulo 3: Se describe el marco teórico que se utiliza en el trabajo.

Capítulo 4: Comprende el desarrollo del proyecto, análisis situacional, alternativa, desarrollo de la solución del problema.

Capítulo 5: Comprende el análisis financiero y resultados de la investigación.

Capítulo 1: Generalidades de la Empresa

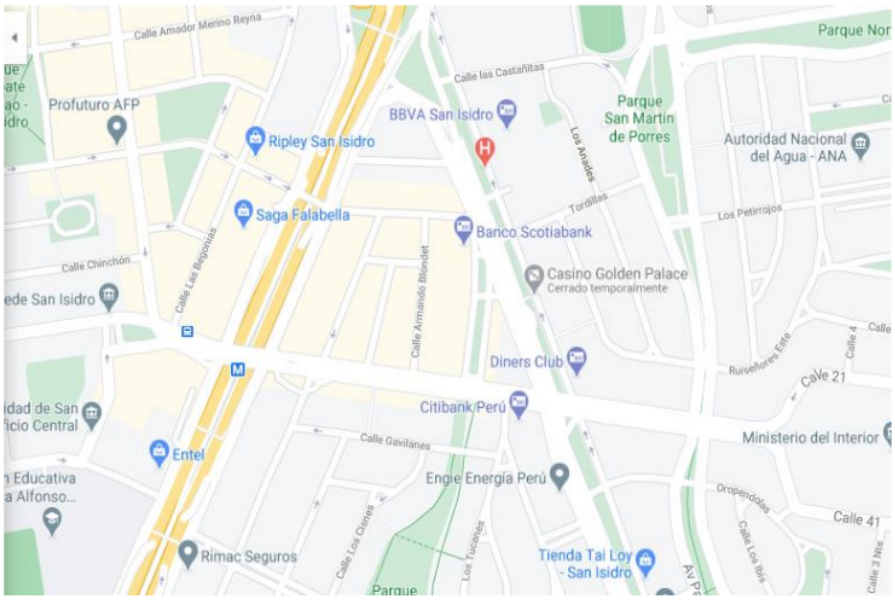
1.1. Datos Generales

La entidad financiera es una empresa privada dedicada a ofrecer servicios de carácter financiero desde el 2004. Asimismo, el banco forma parte del grupo económico liderado por la Caja de Pensiones Militar Policial, institución encargada de la administración del fondo de pensiones del personal de la Policía Nacional del Perú y de las Fuerzas Armadas.

1.2. Ubicación de la empresa

La entidad financiera cuenta con una oficina principal que se encuentra ubicada en el Distrito de San Isidro y Departamento de Lima. También cuenta con 11 agencias en Lima, 7 agencias en las diferentes provincias y 14 oficinas especiales ubicadas en diversas instituciones públicas y privadas.

Figura 1 *Ubicación de la entidad financiera*



Fuente: Google Maps

1.3. Giro de la empresa

Brinda servicios financieros para persona natural y persona jurídica. De acuerdo con la Clasificación Industrial Internacional Uniforme (CIIU), a la entidad financiera le corresponde el código 6419 referido a "Otros tipos de intermediación monetaria".

1.4. Tamaño de la empresa

Según el Ministerio de Economía y Finanzas, la entidad financiera se encuentra clasificada como Gran Empresa debido a que sus ingresos superan los 2,300 UIT según lo establecido por la regulación peruana, tal como se muestra en la tabla 1.

Tabla 1 *Estado de resultados de 2018 y 2019*

Estado de resultados
(expresado en millones de soles)

Rubro	2018	2019	Var. 19-18
Ingreso por intereses	218.6	225.0	6.4
Gasto por intereses	65.2	68.1	2.9
Margen financiero bruto	**153.4**	**156.9**	**3.5**
Provs. para créditos directos	25.1	38.3	13.2
Margen financiero neto	**128.3**	**118.6**	**-9.7**
Ingresos serv. financieros	11.3	14.4	3.1
Gastos serv. financieros	14.4	14.1	-0.4
Margen fin. neto de ing. y gas. por serv.	**125.1**	**118.9**	**-6.2**
Res. por operaciones financieras (ROF)	1.2	3.4	2.2
Margen operacional	**126.3**	**122.3**	**-4.1**
Gastos de administración	72.6	79.6	7.0
Depreciaciones y amortizaciones	7.5	6.4	-1.1
Margen operacional neto	**46.2**	**36.3**	**-9.9**
Valuación de activos y provisiones	3.2	4.3	1.0
Resultado de operación	**43.0**	**32.1**	**-10.9**
Otros ingresos y gastos	-0.1	16.0	16.1
Utilidad a. impuestos	**42.9**	**48.1**	**5.1**
UTILIDAD NETA	**30.8**	**34.6**	**3.8**

Nota: La utilidad neta de la entidad financiera al 2019 ascendió a S/ 34. 6 millones. (Memoria Anual de Banco de Comercio, 2019, p. 25).

1.5. Breve reseña histórica de la empresa

La entidad financiera se dedica a ofrecer servicios financieros tales como la captación de depósito y el otorgamiento de créditos para persona natural y persona jurídica. La

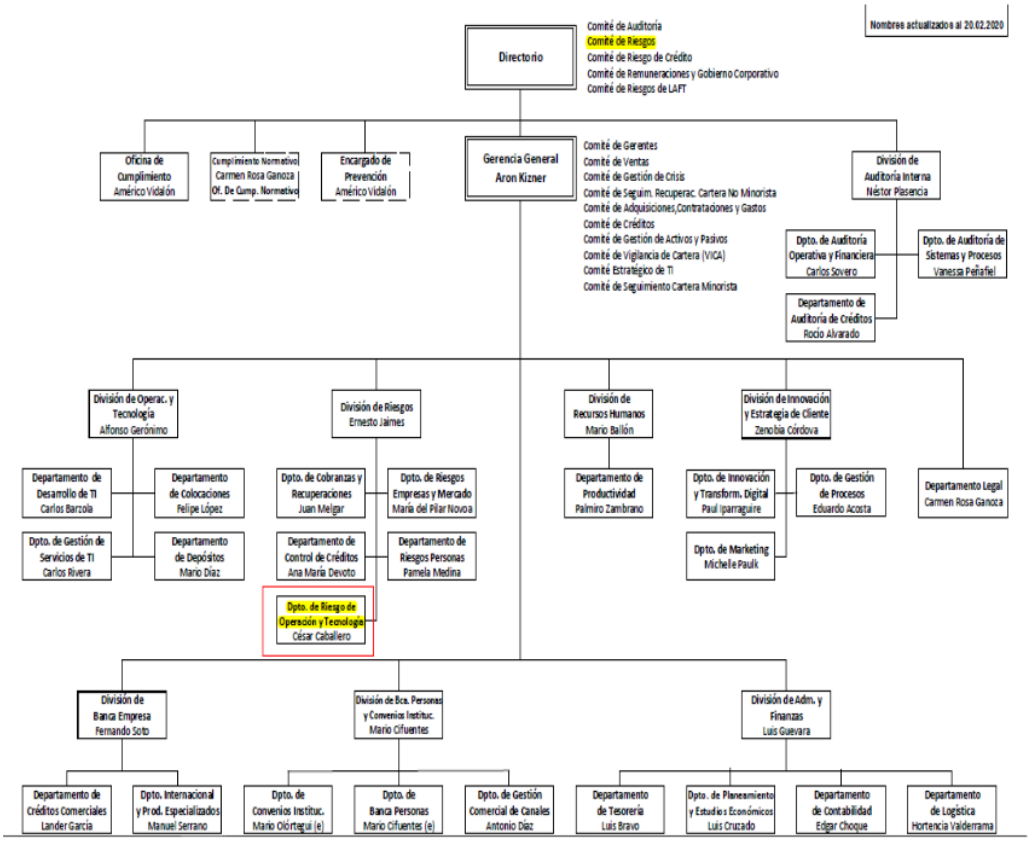
Superintendencia de Banca, Seguros y AFP autorizó su funcionamiento el 27 de agosto de 2004 mediante resolución N° 1466-2004 e inicio sus operaciones el 27 de septiembre de 2004. Tiene como principal accionista la Caja de Pensiones Militar Policial (CPMP), institución que se encarga de la administración del fondo de pensiones del personal de la Policía Nacional del Perú y de las Fuerzas Armadas.

Actualmente, la entidad financiera cuenta con más de 800 colaboradores y con presencia en 09 regiones de nuestro país teniendo 29 agencias de atención a los clientes. Con la finalidad de brindar una mejor experiencia de servicio y adecuarse a las exigencias del mercado, es que, en el 2020 se está impulsando la transformación priorizando aspectos tales como la omnicanalidad, diversificación de los segmentos de las diferentes bancas, fortalecimiento de los procesos que promueva el posicionamiento de la entidad financiera superando las expectativas de los clientes actuales y potenciales. A su vez, se está desarrollando un programa de cambio cultural basado en la innovación y la transformación, el cual permitirá ubicar al cliente en el foco de nuestras decisiones y brindarle productos que le generen una experiencia única.

1.6. Organigrama de la empresa

La entidad financiera cuenta con un organigrama estructural que nace desde el Directorio y Gerencia General y se extiende en las diferentes divisiones, departamentos y unidades de mando, la cual permite cumplir con los objetivos y metas institucionales. La estructura organizacional se encuentra organizada de la siguiente manera:

Figura 2 *Organigrama Estructural*



Fuente: Intranet de la Entidad Financiera

En la figura 2, se puede observar la División de Riesgos, donde se encuentra el Departamento de Riesgo de Operación y Tecnología. Cabe precisar que está considerada como un área de control y es la segunda línea de defensa en la organización.

A continuación, se detallan las funciones de las divisiones de la entidad financiera:

Oficina de Cumplimiento

Tiene como función vigilar el correcto funcionamiento del Sistema de Prevención y Gestión de los Riesgos de Lavado de Activos y del Financiamiento del Terrorismo y del

Programa de Prevención de Corrupción con el objetivo de reducir riesgos del movimiento ilícito de capitales y de corrupción en la entidad financiera.

Cumplimiento Normativo

Se encarga de vigilar el cumplimiento de las normativas y requerimientos regulatorios.

División de Auditoría Interna

Se encarga de evaluar la eficacia y eficiencia del Sistema de Control Interno. Asimismo, evalúa y recomienda mejora en los procesos de gestión de riesgos, control y gobierno corporativo.

División de Riesgos

Tiene como función el cumplimiento de una adecuada Gestión Integral de Riesgos, permitiendo identificar, evaluar, tratar, controlar y reportar los riesgos. Está compuesta por riesgos financieros y no financieros. Los riesgos financieros están orientados a identificar, evaluar y controlar los riesgos crediticios, mercado, liquidez y país. Los riesgos no financieros son los sistemas de gestión de riesgo operacional, donde se incluye la gestión de continuidad del negocio y seguridad de la información.

División de Operación y Tecnología

Se encarga de brindar un adecuado, eficiente y oportuno soporte operativo a los productos y servicios financieros. Asimismo, brinda un óptimo servicio de tecnología de información, garantizando un adecuado uso de los recursos tecnológicos.

División de Recursos Humanos

Se encarga de velar por la correcta administración del personal, reclutamiento y selección, clima laboral, productividad y remuneración.

División de Innovación y Estrategia de Cliente

Encargada de dirigir los modelos de negocio innovadores y rentables, desarrollar estrategia de marketing para fortalecer la imagen de la entidad financiera y organizar la gestión de procesos a través del desarrollo de normativas.

División de Banca Empresa

Se encarga de fomentar las actividades de negocio de la cartera de clientes jurídicos de los diversos sectores empresariales, inmobiliarios e institucionales, con el objetivo de cumplir las metas de colocación y captación.

División de Banca Personas y Convenios Institucionales

Tiene como función fomentar las actividades de negocio de la cartera de clientes naturales de los sectores de las Fuerzas Armadas, Policía Nacional del Perú, así como los negocios de personas naturales, con el objetivo de cumplir las metas de colocación y captación.

División de Administración y Finanzas

Se encarga de planear, dirigir, coordinar, controlar el funcionamiento del plan estratégico y el presupuesto anual, así como la administración de todos los recursos financieros. Asimismo, se encarga de la gestión de logística, seguridad y administrar el sistema contable y tributario.

1.7. Misión, Visión y Propósito

Misión

"Brindar soluciones financieras innovadoras, ágiles y accesibles".

Visión

"Ser reconocidos por ofrecer la más memorable de las experiencias en servicios financieros".

Propósito

"Impulsamos el poder de quienes persiguen sus sueños".

Valores

La entidad financiera cuenta con los siguientes valores:

- Colaboración y empoderamiento: Para construir una organización más horizontal con equipos autogestionados y autoorganizados que desarrollen mejores procesos, productos y servicios.
- Resiliencia e Innovación: Para sobreponernos a situaciones adversas, aprender de los errores y mejorar continuamente y de manera innovadora aprovechar las oportunidades.
- Empatía y orientación al cliente: Para entender y conocer a las personas conectando con sus necesidades y sueños con ofertas de alto valor.
- Ética e Integridad: Actuamos con fidelidad a nuestros principios, respetando a los colaboradores, accionistas, clientes, proveedores y entes reguladores.

1.8. Productos y Clientes

La entidad financiera cuenta con una cartera diversa de productos activos y pasivos para persona natural y persona jurídica, tal como se muestra en la siguiente tabla.

Tabla 2 *Productos de la entidad financiera*

	Banca Persona	Banca Empresa
Productos Activos	Préstamo Personal	Descuento de Facturas Electrónicas
	Crédito con garantía en joyas	Descuento de Letras y Pagarés
	Crédito Mivivienda	Leasing
	Préstamo Convenio P.N.P	Capital de Trabajo
	Préstamo Convenio Marina de Guerra	Financiamiento de Ventas
	Préstamo Convenio Fuerza Áerea del Perú	Financiamiento de Comercio Exterior (import/export)
		Financiamiento Mediano Plazo

	Préstamo Convenio Ejército del Perú	Programa Reactiva Perú
	Tarjeta de Crédito	Tarjeta Visa Empresarial
Productos Pasivos	MaxiCTS	Ahorro Empresas
	MaxiPlazo	
	Plan Ahorro Junta	
	MaxiAhorro Preferencial	Depósito a Plazo Empresas
	Ahorro Tradicional	
	Cuenta Sueldo	

Nota: Adaptado de la intranet de la entidad financiera.

Dentro de los principales clientes se encuentran los beneficiarios de los convenios institucionales con las Fuerzas Armadas y la Policía Nacional del Perú.

1.9. Relación de la empresa con la sociedad

De acuerdo con el análisis realizado por Pacific Credit Rating (PCR), la entidad financiera tiene un nivel de desempeño bueno catalogado como RSE3 respecto a la responsabilidad social empresarial, donde RSE1 es la categoría máxima y RSE6 es la mínima. A través de los años, se fomentó la responsabilidad social empresarial y se estableció un vínculo de cooperación y apoyo. Se realizó las siguientes actividades de ayuda social:

- Participó y apoyó en el concierto benéfico que realizó la Asociación Stella Maris, institución de bien social sin fines de lucro conformado por las esposas de oficiales de la Marina de Guerra del Perú. Esto con la finalidad de que los fondos estuvieran destinados a la remodelación del área de Unidad de Cuidados Intensivos Neonatales del Centro Médico Naval "Cirujano Mayor Santiago Távara".
- La Unidad de Bienestar Social desarrollo la campaña "Destapa una Sonrisa", el cual consiste en la recolección de tapas de plástico que serán donadas al programa "Angelitos de Cristal" auspiciado por el Instituto Nacional de Salud

del Niño a fin de apoyar en el tratamiento de los niños que sufren de epidermólisis bullosa.

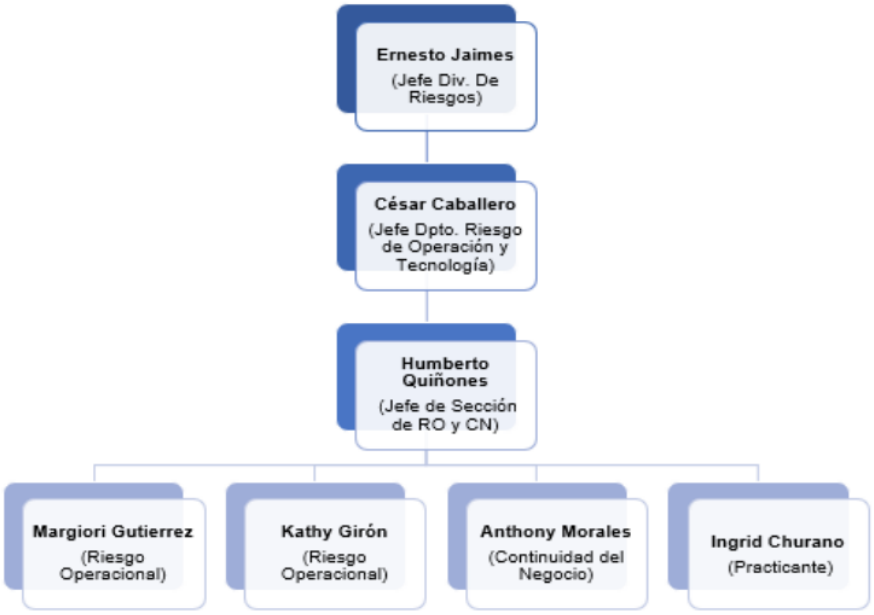
- Se realizaron donativos a las Fuerzas Armadas y Policía Nacional del Perú por motivo de fiestas navideñas, día del padre y de la madre.

Capítulo 2: Planteamiento del Problema

2.1. Caracterización del Área

El área de Riesgo Operacional se enfoca en brindar apoyo y la asesoría a todas las unidades de negocio y de apoyo de la entidad financiera para una adecuada gestión de riesgo operacional, dicha gestión se fundamenta en políticas, metodologías y procedimientos aprobados por el Comité de Riesgos dentro del marco del Sistema de Gestión Integral de Riesgos (GIR). El departamento de Riesgo Operacional se encuentra conformada de la siguiente manera, tal como se muestra en la figura 3.

Figura 3 *Estructura de Riesgo Operacional*



Fuente: Elaboración propia.

Cabe precisar que es la segunda línea de defensa debido a que realizan la supervisión de riesgos, controles y cumplimiento, siendo la primera línea de defensa las gerencias

propietarias y/o dueñas del proceso que tienen los riesgos y los gestionan, y la tercera línea de defensa bajo el cargo de auditoría interna que se encarga del aseguramiento de los riesgos.

Figura 4 *Modelo de las tres líneas de defensa*

Fuente: Adaptado de la Guía emitida por ECIIA/FERMA sobre la 8va Directiva de Derecha de Sociedades de la Unión Europea

Asimismo, la Gestión de Riesgo Operacional está asociada a los procesos de la entidad financiera, por ello cada proceso debe ser analizado con el objetivo de identificar riesgos operacionales que provienen de los cuatro factores (personas, procesos internos, tecnología de la información y eventos externos) y poder evaluar el nivel de riesgo a los que se encuentra expuesto y los controles con la finalidad de tomar acciones y/o medidas para mitigar la exposición del riesgo.

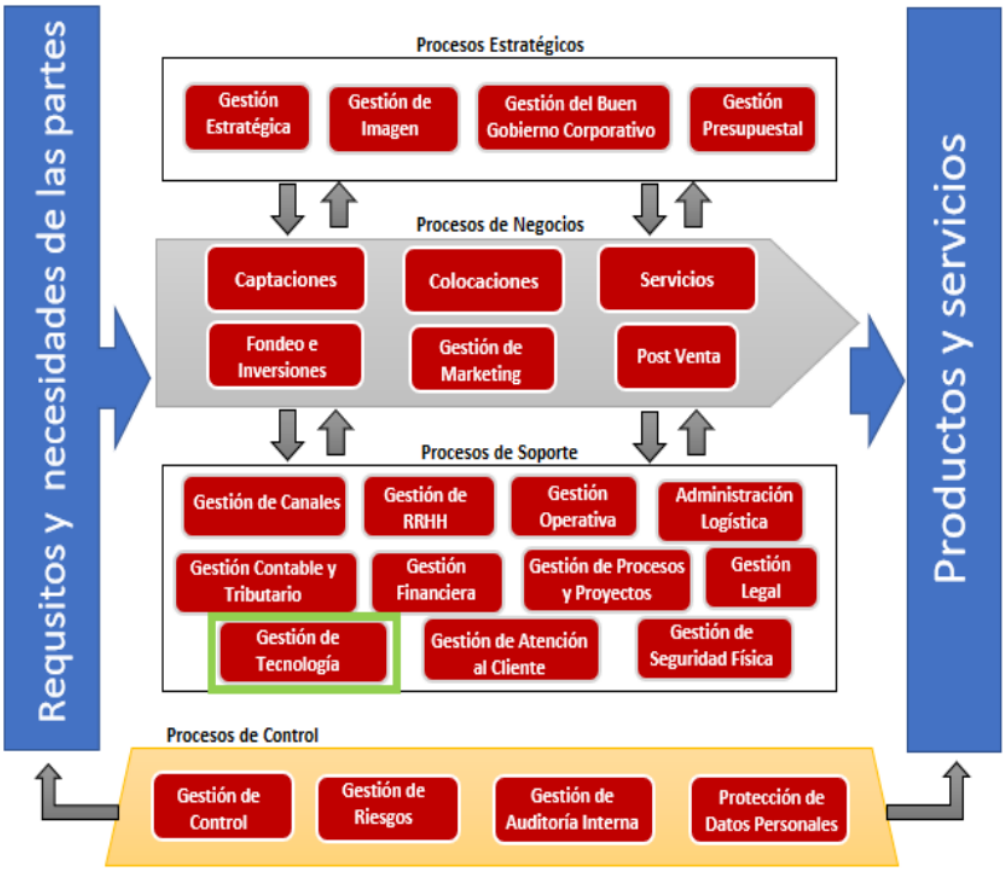
Por ello, la entidad financiera cuenta con un mapa de procesos que recoge la interrelación de todos los procesos y permite tener una correcta administración de gestión de la empresa.

Es preciso mencionar que un mapa de procesos es la estructura donde se representa la interrelación de los procesos estratégicos, de negocio, soporte y control que posee una

empresa. Asimismo, brinda una visión sistémica y refleja la realidad de la empresa y esta debe ser fácil de comunicar y comprender (Pérez, 2004).

El mapa de proceso de la entidad financiera se muestra en la siguiente figura, a su vez el Departamento de Procesos tiene la responsabilidad de velar que las normativas internas se encuentren actualizados.

Figura 5 *Mapa de procesos de la entidad financiera*



Fuente: Elaboración propia. Adaptado del "Inventario de procesos", por la entidad financiera. (2019)

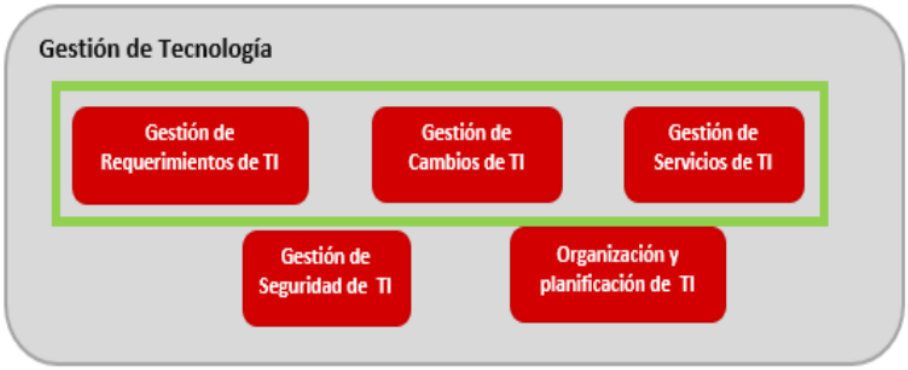
Los procesos estratégicos son establecidos por la alta dirección, con el objetivo de ofrecer soporte para la toma de decisiones en relación con la planificación y estrategias en la entidad financiera. Los procesos del negocio están relacionados a los servicios que presta en

beneficio al cliente, estos generan valor. Los procesos de soporte son aquellos fundamentales que sirven de apoyo a los procesos del negocio y los procesos de control permiten vigilar el cumplimiento de las normativas de los entes reguladores y evaluar la eficacia o eficiencia de los demás procesos.

Por otro lado, se involucra la participación de todas las áreas de la organización, cada una de ellas con diversas funciones y responsabilidades que permiten un adecuado control de los riesgos operacionales que se encuentra expuesta la entidad financiera. Para ello, se estableció contar con un grupo de gestores y coordinadores de riesgos, quienes son los funcionarios representantes del dueño de los procesos a su cargo, son responsables de participar en las metodologías de gestión de riesgo operacional.

En el presente trabajo de suficiencia profesional se realizará el análisis del proceso de soporte "Gestión de Tecnología", el cual comprende desde la Gestión de Requerimiento de TI, Gestión de Cambios de TI y la Gestión de Servicios de TI.

Figura 6 *Proceso de Gestión de Tecnología de la entidad financiera*



Fuente: Elaboración propia. Adaptado del "Inventario de procesos", por la entidad financiera. (2019)

2.2. Contextualización y Definición del Problema

2.2.1. Contextualización del Problema

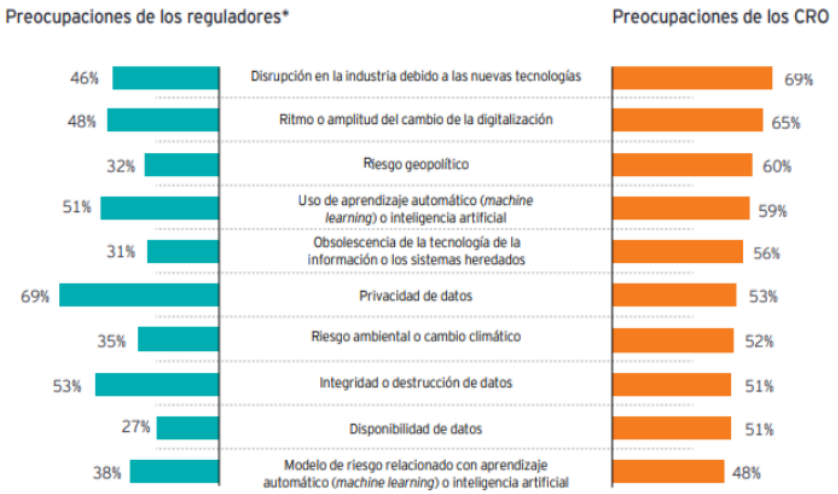
En el Perú, las instituciones financieras están reguladas por la Superintendencia de Banca, Seguros y AFP (SBS), la cual exige administrar los riesgos operacionales asociados con los procesos basado en el Reglamento para la Gestión de Riesgo Operacional Resolución S.B.S. N° 2116-2009.

En la actualidad, la revolución tecnológica se ha vuelto imprescindible para la conservación de una empresa. Es por ello, que el sector financiero está enfrentando muchos cambios tecnológicos y frente a ellos nos encontramos ante cambios en los procesos y expuestos a diversos riesgos. Por lo tanto, la gestión de riesgos es fundamental en un proceso de transformación. Las entidades financieras están buscando oportunidades de mejora adquiriendo tecnologías innovadoras que se adapten al negocio tales como; la computación en nube, inteligencia artificial, canales digitales, fintech, entre otras, para satisfacer las necesidades del negocio y controlar las operaciones facilitando la toma de decisiones.

En un estudio publicado "¿Es la ética el gran dilema del siglo XXI?" por Ernst & Young, destaca que los principales riesgos que se deben considerar en la industria financiera bajo un entorno de transformación digital deben ser los relacionados a la protección de la información, disponibilidad y confiabilidad de TI, cybersecurity, cloud computing, gestión de licencias y softwares, entre otros.

Asimismo, en la siguiente figura 7 se puede visualizar los riesgos que serán prioridad de los reguladores y de los encargados de la gestión de riesgos de las entidades financieras. Entre ellos se destaca los riesgos relacionados a la privacidad de datos, integridad de datos, disponibilidad de datos, obsolescencia de la tecnología; las cuales están relacionadas con el proceso de Gestión de Tecnología.

Figura 7 *Prioridades de los reguladores y de los CRO a largo plazo*



Fuente: Informe de EY

La entidad financiera en estudio tiene como objetivo la implementación de los productos mediante canales digitales, a fin de poder brindar al cliente un canal adicional para adquirir los productos y así tener mayor llegada a los clientes. Para ello, es necesario que la entidad financiera implemente controles y medidas de seguridad en el proceso de gestión de tecnología debido a que si los riesgos se manejan de forma inadecuada podría repercutir en un riesgo reputacional generando desconfianza a los clientes.

Por lo expuesto, el Departamento de Riesgo de Operación y Tecnología propuso realizar el análisis y evaluación al proceso de Gestión de Tecnología, ya que es un proceso de soporte fundamental para el desarrollo de los procesos principales del negocio. Esto permitirá conocer el nivel y exposición de riesgo que están dispuestos de aceptar y determinar el alcance para la mitigación de estos.

2.2.2. Formulación del Problema

Problema General

¿Cómo la aplicación de la metodología de riesgo operacional mejora el proceso de gestión de tecnología en una entidad financiera?

Problemas Específicos

¿Cuáles son las metodologías de riesgo operacional que se utilizarán para el análisis del proceso de gestión de tecnología en una entidad financiera?

¿Cómo se identificará y evaluará los riesgos operacionales para determinar el nivel de exposición inherente del proceso de gestión de tecnología en una entidad financiera?

¿Cómo se identificará la evaluación de los controles del proceso para determinar el nivel de exposición residual del proceso de gestión de tecnología en una entidad financiera?

¿Cuáles son los indicadores que se utilizarán para monitorear los riesgos operacionales del proceso de gestión de tecnología en una entidad financiera?

¿Cuáles son los planes de acción que se utilizarán para mitigar los riesgos operacionales del proceso de gestión de tecnología en una entidad financiera?

2.3. Objetivos

2.3.1. Objetivo General

Mejorar el proceso de gestión de tecnología en una entidad financiera aplicando metodologías de riesgo operacional.

2.3.2. Objetivos Específicos

Determinar las metodologías de riesgo operacional a utilizar para el análisis del proceso de gestión de tecnología en una entidad financiera.

Identificar y evaluar los riesgos operacionales para determinar el nivel de exposición inherente del proceso de gestión de tecnología en una entidad financiera.

Identificar y evaluar los controles del proceso para determinar el nivel de exposición residual del proceso de gestión de tecnología en una entidad financiera.

Establecer indicadores que se utilizarán para monitorear los riesgos operacionales del proceso de gestión de tecnología en una entidad financiera.

Establecer los planes de acción que se utilizarán para mitigar los riesgos operacionales del proceso de gestión de tecnología en una entidad financiera.

2.4. Justificación

El presente trabajo se justifica desde el punto de vista del criterio teórico, práctico y social. Estos criterios nos ayudarán para adquirir nuevos conocimientos relacionados al tema o resolver los problemas con los que cuenta la empresa.

Desde el punto de vista teórico, el presente trabajo brindará información relevante de la aplicación de la metodología de riesgo operacional realizada al proceso de gestión de tecnología en las entidades financieras mediante la autoevaluación de riesgos y controles del proceso.

Desde el punto de vista práctico, el presente trabajo se realiza en una entidad financiera con la finalidad de dejar como base la mejora realizada al proceso de gestión de tecnología. Además de poder mitigar los riesgos a los que se encuentra expuesto dicho proceso y evitar la materialización de los eventos operacionales.

Desde el punto de vista social, el presente trabajo ayuda a fortalecer el trabajo colaborativo debido a que motiva a los colaboradores de la entidad financiera en la detección oportuna de riesgos y mejoramiento continuo de los controles. Además, mejora la comunicación en todos los niveles debido a que los talleres se realizan con equipos multidisciplinarios. Finalmente, permite a la entidad financiera generar mayor confianza en sus clientes debido a que los riesgos operacionales asociados se estarían gestionando de forma adecuada.

2.5. Alcances y Limitaciones

El resultado del presente trabajo ayudo a mejorar el proceso de gestión de tecnología debido a la evaluación de riesgos y controles, por ello el alcance comprende solo la evaluación de 03 procesos de Gestión de Tecnología, los cuales son:

- Gestión de Requerimientos de TI, el proceso consiste en la recepción, análisis y la gestión de atención de los requerimientos relacionados de tecnología de la información de los usuarios del banco correspondientes a soporte técnico, requerimientos de desarrollo de sistemas. Asimismo, también se gestiona las posibles incidencias que se presenten.
- Gestión de Cambios de TI, el proceso consiste en controlar y gestionar el ciclo de vida de un desarrollo de sistema, teniendo en cuenta la fase de construcción o desarrollo, control de calidad, pase a producción del sistema y el control de versiones de fuentes y programas. Asimismo, el objetivo del proceso es mitigar el riesgo y el impacto, así como la reducción de incidencias debido a la ejecución de los cambios.
- Gestión de Servicios TI, este proceso se encarga de gestionar, administrar de forma eficiente los recursos y monitorear los servicios de tecnología incluido los servicios de proveedores.

Es preciso indicar que la última actualización del mapa de procesos fue en el 2018, esto sirvió como guía para el desarrollo del trabajo.

Asimismo, el trabajo está elaborado con los datos de la entidad financiera; sin embargo, por motivos de confidencialidad no se utilizará el nombre de la organización.

Capítulo 3: Marco Teórico

En el presente capítulo se dará a conocer los conceptos relacionados a riesgo operacional y gestión de tecnología.

3.1. Superintendencia de Banca, Seguros y AFP

(La Superintendencia de Banca, Seguros y AFP [SBS],2019) es el organismo público que se encarga de la regulación y supervisión de las entidades financieras, seguros y del sistema privado de pensiones, así como prevenir y detectar el lavado de activos y financiamiento del terrorismo.

3.2. Gestión Integral de Riesgos

La Superintendencia de Banca, Seguros y AFP mediante la resolución SBS N° 272, sostiene que:

La Gestión Integral de Riesgos es un proceso efectuado por el directorio, la gerencia y el personal aplicado a toda la empresa y en la definición de su estrategia, diseñado para identificar potenciales eventos que pueden afectarla, gestionarlos de acuerdo con su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos. La Gestión Integral de Riesgos incluye la totalidad de la empresa, sus líneas de negocio, procesos y unidades organizativas, a través de todos sus riesgos relevantes. Las empresas deben diseñar y aplicar una gestión integral de riesgos, adecuada a su naturaleza, tamaño y a la complejidad de sus operaciones y servicios, así como al entorno macroeconómico que afecta a los mercados en los que opera la empresa. (2017, p. 14).

3.3. Riesgo

COSO ERM define el riesgo como “la posibilidad de que un evento ocurra y afecte adversamente el logro de los objetivos” (2004, p. 16).

3.4. Riesgo Operacional

La SBS define el riesgo operacional como "La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación" (2017).

3.5. Factores que originan el riesgo operacional

De acuerdo con la Resolución SBS N° 2116- 2009 hace hincapié que existen factores internos y externos que podrían originar riesgos en la organización. Asimismo, sostiene que:

Procesos internos

Las empresas deben gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos. (2009, p.5).

Personal

Las empresas deben gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros. (2009, p.5).

Tecnología de información

Las empresas deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos. (2009, p.5).

Eventos externos

Las empresas deberán gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores. (2009, p.5).

3.6. Evento de riesgo operacional

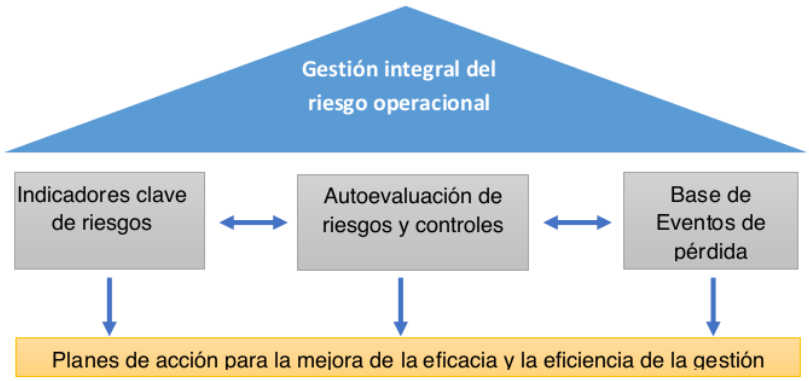
Manual de Políticas y Procedimientos Sistema de Gestión de Riesgo Operacional indica que un evento de riesgo operacional "es un suceso o series de sucesos derivados de los factores de Riesgo Operacional originados por la(s) misma(s) causa(s), que ocurren durante un periodo de tiempo, afectando el curso normal de los procesos del Banco." (2019, p. 4)

Alexander et al. Sostiene que "los eventos de riesgo operacional se caracterizan por dos parámetros: impacto y frecuencia." (2010, p.185)

3.7. Metodología de la Gestión de Riesgo Operacional

Las metodologías de la Gestión de Riesgo Operacional tienen un enfoque cualitativo y cuantitativo, en la siguiente figura se puede observar la interrelación que existe entre ellas.

Figura 8 *Gestión integral del riesgo operacional*



Fuente: Elaboración propia. Adaptado de "La gestión de riesgo operacional: de la teoría a su aplicación", por Alexander et al. (2010)

Indicadores clave de riesgos

Los indicadores clave de riesgos son datos estadísticos y métricos que permiten conocer la posición de riesgos de la organización y tomar medidas correctivas y oportunas ante alguna desviación de parámetros. Asimismo, cumple una función de señal de alerta temprana que notifica cuando algo no está funcionando como debería. (Alexander et al., 2010).

Autoevaluación de riesgos y controles

La metodología de autoevaluación de riesgos y controles consiste en la identificación de los riesgos, los cuales se evalúan en función a la probabilidad de ocurrencia y el impacto que pueda generar. Asimismo, se identifican y evalúan los controles y según el nivel de riesgo obtenido se establecen medidas correctivas para mitigarlos. (Alexander et al., 2010).

Análisis de Riesgos

El Ministerio de Hacienda y Administraciones Públicas explica que "busca calificar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis cualitativo). De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante" (2012, p. 20). De acuerdo con el texto el análisis de riesgo permite averiguar el nivel de riesgo que la empresa está sobrellevando.

Tratamiento de los riesgos

El Ministerio de Hacienda y Administraciones Pública afirma que:

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario (2012, p.10).

En resumen, existen varios tipos de tratamiento de riesgo que se da para aquellos riesgos cuyo nivel están por encima del límite deseado de la organización.

Base de evento de pérdida

Alexander et al. Explica que "una pérdida por riesgo operacional es todo impacto negativo en la cuenta de resultados o en el patrimonio (activos) de la entidad como consecuencia de un factor de riesgo operacional." (2010, p.343).

Alexander et al. Indica que una base de eventos de pérdida "debe permitir capturar, autorizar y realizar un seguimiento adecuado de los eventos o sucesos de riesgo operacional que se producen en cada entidad, conocer el número y nivel de pérdidas, mitigar las mismas y, posteriormente cuantificar el capital mediante un modelo avanzado." (2010, p.307).

3.8. Proceso

Se entiende como proceso "cualquier actividad o grupo de actividades mediante las cuales uno o varios insumos son transformados y adquieren un valor agregado, obteniéndose así un producto para un cliente" (Krajewski & Ritzman, 2000, p.8)

La mayoría de las entidades financieras, dividen en macroprocesos, procesos y subprocesos respectivamente. La entidad financiera cuenta con 04 macroprocesos, los cuales son los estratégicos, negocios, soporte y de control. En el presente trabajo se evaluará el proceso de Gestión de Tecnología. Es preciso indicar que, para implementar la Gestión de Riesgo Operacional, el proceso debe estar definido y contar con su diagrama de flujo, con el objetivo que a partir de ahí se realiza el análisis correspondiente.

Alexander et al. explica que "los procesos están expuestos a una gran variedad de riesgos que pueden provocar que el resultado esperado no se produzca como se planeó originalmente, Puede haber errores, averías informáticas, huelgas, inundaciones, fraudes, es decir, un sinfín de circunstancias que generan costes adicionales no previstos, ineficiencias, pérdidas de negocio, etc" (2010, p.182)

3.9. Procedimiento

ITIL indica que la gestión de cambios “Es un documento que contiene pasos que especifican cómo llevar a cabo una actividad. Los procedimientos se definen como parte de los procesos.” (2011, p. 79)

3.10. Gestión de Tecnología

Jaimes, Ramirez, Vargas y Carrillo explican que la gestión de tecnología “es un conjunto sistemático de procesos orientados a la planificación, organización y ejecución de actividades relacionadas con la evaluación, adquisición y puesta en marcha de tecnologías claves para el cumplimiento de los objetivos estratégicos de una organización; con el objetivo de generar productos y/o servicios competitivos.” (2011)

3.11. Tecnología de la Información

La tecnología de la información se refiere al uso de equipos tecnológicos (computadoras, telecomunicaciones y aplicaciones) para la comunicación, procesamiento y almacenamiento de la información. Es preciso indicar que la tecnología de información es necesaria para apoyar los procesos del negocio a través de los servicios de TI. (ITIL® Español (Latinoamericano) Glosario V1.0, 2011)

3.12. Gestión de Cambios de TI

ITIL explica que un cambio “consiste en añadir, modificar o eliminar cualquier cosa que pudiera tener un efecto en los servicios de TI.” (2011, p. 21)

Asimismo, ITIL también indica que la gestión de cambios “es el proceso responsable de controlar el ciclo de vida de todos los cambios, permitiendo que se realicen cambios que son beneficiosos, minimizando la interrupción de servicios de TI.” (2011, p. 22)

3.13. Gestión de Servicios TI

ITIL indica que la gestión de servicios TI "es la implementación y gestión de la calidad de los servicios de TI que cumplan las necesidades del negocio. La gestión de servicios de TI se lleva a cabo por los proveedores de servicios de TI a través de una combinación adecuada de personas, procesos y tecnología de información." (2011, p. 61)

3.14. Incidente TI

ITIL explica que el incidente es "una interrupción no planificada de un servicio de TI o la reducción en la calidad de un servicio de TI." (2011, p. 54)

Capítulo 4: Desarrollo del Proyecto

4.1. Análisis Situacional

Se realizó un análisis FODA que permitió identificar las fortalezas y debilidades de la entidad financiera, con el objetivo de establecer estrategias ante las oportunidades de crecimiento y amenazas que se presenten en el mercado. En la siguiente figura, se muestra el resultado del análisis interno y externo que se identificó.

Figura 9 *Análisis FODA*

Fuente: Elaboración propia.

La entidad financiera tiene un entorno favorable debido a los cambios y avances tecnológicos se tiene como objetivo la implementación de productos mediante los canales digitales y así poder llegar al nuevo segmento de clientes. Por ello, la alta dirección decidió incrementar el presupuesto de TI con la finalidad de mejorar todo el proceso de la gestión de tecnología.

Asimismo, se analizó la situación y se evaluó los factores internos y externos a través de la matriz EFE y EFI que inciden en la gestión de la tecnología de la entidad financiera, lo cual permitió identificar los puntos críticos que afectan a los objetivos de TI.

Tabla 3 *Matriz EFE de Gestión de Tecnología*

	Factores Críticos para el éxito	Peso	Calificación	Total Ponderado
N°	**Oportunidades**			
1	Innovación de productos y canales	20%	4	0.80
2	Avances de la tecnología	12%	3	0.36
3	Regulación SBS	15%	3	0.45
4	Nuevo segmento de clientes	15%	3	0.45
N°	**Amenazas**			
1	Incremento de fraudes y ciberataques	12%	3	0.36
2	Oferta laboral en otras financieras	8%	3	0.24
3	Falta de adecuación cambios tecnológicos	5%	1	0.05
4	Aparición de competidores	8%	1	0.08
5	Incremento en el costo de tecnología	5%	2	0.10
	TOTAL	100%		2.89

Nota: Calificación de los factores externos en base al análisis foda del trabajo de suficiencia profesional. Elaboración propia.

El resultado de las ponderaciones de la matriz EFE es de 2.89, el cual está por encima del promedio (2.50), lo que significa que la gestión de tecnología tiene muchas oportunidades de seguir mejorando, por lo cual la estrategia debe apuntar a las alternativas de solución que permitan mitigar el impacto o evitar las amenazas latentes.

Entre las principales oportunidades de mayor peso, se identificaron 03 factores importantes:

- Innovación, mejora de los productos a través de la implementación de los canales digitales, permite enfocarnos al nuevo segmento de clientes.
- La regulación de la SBS se está enfocando en la gestión de las áreas de TI.
- El nuevo segmento de clientes de la entidad financiera, son los jóvenes que tienen mayor conexión con la tecnología.

Tabla 4 *Matriz EFI de Gestión de Tecnología*

	Factores Críticos para el éxito	Peso	Calificación	Total Ponderado
N°	**Fortalezas**			
1	Compromiso de la alta dirección	15%	4	0.60
2	Incremento de presupuesto TI	15%	4	0.60
3	Alianza con proveedores	10%	3	0.30
4	Personal comprometido y capacitado	10%	3	0.30
5	Baja rotación de personal	8%	3	0.24
6	Disposición de recursos para fortalecer los procesos	10%	3	0.30
N°	**Debilidades**			
1	Ausencia y desactualización de procedimientos	10%	1	0.10
2	Deficiente coordinación entre las áreas y proveedor	8%	1	0.08
3	Falta de control y monitoreo a los procesos	8%	1	0.08
4	Falta de definición de responsabilidades	6%	2	0.12
	TOTAL	100%		2.72

Nota: Calificación de los factores internos en base al análisis foda del trabajo de suficiencia profesional. Elaboración propia.

El resultado de las ponderaciones de la matriz EFI es de 2.72, el cual está por arriba del promedio (2.50), lo que significa que la empresa es fuerte de forma interna, pero se debe establecer estrategias que apunten a fortalecer las debilidades encontradas.

Las debilidades con mayor calificación ponderada son las siguientes:

- Ausencia, deficiencia y desactualización de los procedimientos relacionados a Gestión de Tecnología.
- Deficiente coordinación de las actividades entre las áreas internas de TI y Procesos.
- Falta de control y monitoreo a los procesos internos relacionados a Gestión de Tecnología, así como también el monitoreo a los proveedores externos que tienen actividades de soporte.
- Falta de definición de responsabilidades del personal interno y externo relacionado al proceso de Gestión de Tecnología.

Asimismo, las principales fortalezas que se detectaron son:

- Compromiso por parte de la alta dirección respecto a la Gestión de Riesgos y Gestión de TI.
- Incremento del presupuesto para el área de TI, permite mejorar los recursos, procesos involucrados para ofrecer un mejor soporte tecnológico a las distintas áreas de la entidad financiera.
- El personal que se tiene está comprometido y capacitado en sus funciones y también sobre las metodologías de riesgos.

Cabe precisar que se tiene como visión el cambio de transformación digital e innovación, teniendo en cuenta como primera fase la aplicación de canales digitales para los productos de la entidad financiera, con el objetivo de mejorar el valor al cliente. Por lo indicado resulta oportuno implementar controles en el proceso de gestión de tecnología debido a que si los riesgos se manejan de forma inadecuada podría repercutir en un riesgo operacional y reputacional.

Por otro lado, al no haberse gestionado el proceso de documentación, los respectivos procedimientos del proceso de gestión de tecnología no se encuentran actualizados y no se tiene definida la estructura y responsabilidades del personal, debido a que en el último trimestre de 2018 y primer trimestre de 2019 se realizó la tercerización de algunos servicios tecnológicos. Asimismo, con esta tercerización se logró una alianza con el proveedor de Telefónica del Perú, el cual es considerado como proveedor crítico y subcontratación significativa.

Además, se realizó una revisión a la base de incidencias de riesgo operacional y a la base de datos de eventos de pérdida donde se identificó que se presentaron eventos operacionales que generaron pérdidas afectando a los estados financieros. Cabe precisar que en esta revisión se consideró la variable de impacto que va en relación con el monto de pérdida ocasionado a la entidad financiera. Durante el periodo de agosto de 2018 al cierre de julio de 2019 (periodo de un año) se tuvo una pérdida por el monto de S/ 309,853.24 representando un total de 24 eventos de pérdida debido al factor de tecnología de información. Asimismo, se tuvo un total de 35 eventos operacionales que no generaron pérdida en el factor de tecnología.

Figura 10 *Pérdida de Riesgo Operacional - TI*

Fuente: Elaboración propia. Adaptado de la "Base de Eventos de Pérdida", por la entidad financiera. (2019)

Cabe precisar que un evento de riesgo operacional no solo podría ocasionar pérdida monetaria, también puede dar lugar a reflejarse en reclamos de clientes inclusive consecuencias legales o se podría tener sanciones por parte de los entes reguladores del sector financiero.

4.2. Alternativa de Solución

Luego de analizar los problemas que se tienen en el proceso de gestión de tecnología, donde se comprueba que los procedimientos relacionados se encuentran desactualizados y/o no están bien establecidos. El equipo del Departamento de Riesgo de Operación y Tecnología propuso realizar el análisis y evaluación al proceso debido a que es un proceso de soporte fundamental para el desarrollo de los procesos principales del negocio. Esto permitirá mejorar el proceso a través del fortalecimiento de los controles, conocer el nivel y exposición de riesgo que están dispuestos de aceptar y determinar el alcance para la mitigación de estos. Asimismo, permitirá monitorear los riesgos extremos y altos mediante indicadores clave de riesgos.

4.3. Desarrollo de la solución del problema

4.3.1. Metodologías de la Gestión de Riesgo Operacional

Se aplicarán las metodologías de riesgo operacional a fin de lograr la mejora del proceso de gestión de tecnología.

Por ello, se determinó aplicar las siguientes metodologías:

- Metodología de Autoevaluación de Riesgos y Controles, la cual comprende el entendimiento del proceso, la identificación, evaluación de los riesgos inherentes (utilizando la frecuencia e impacto), evaluación de los controles con que cuentan los riesgos y así poder determinar el nivel de riesgo residual a los que se encuentra expuesto el proceso evaluado.

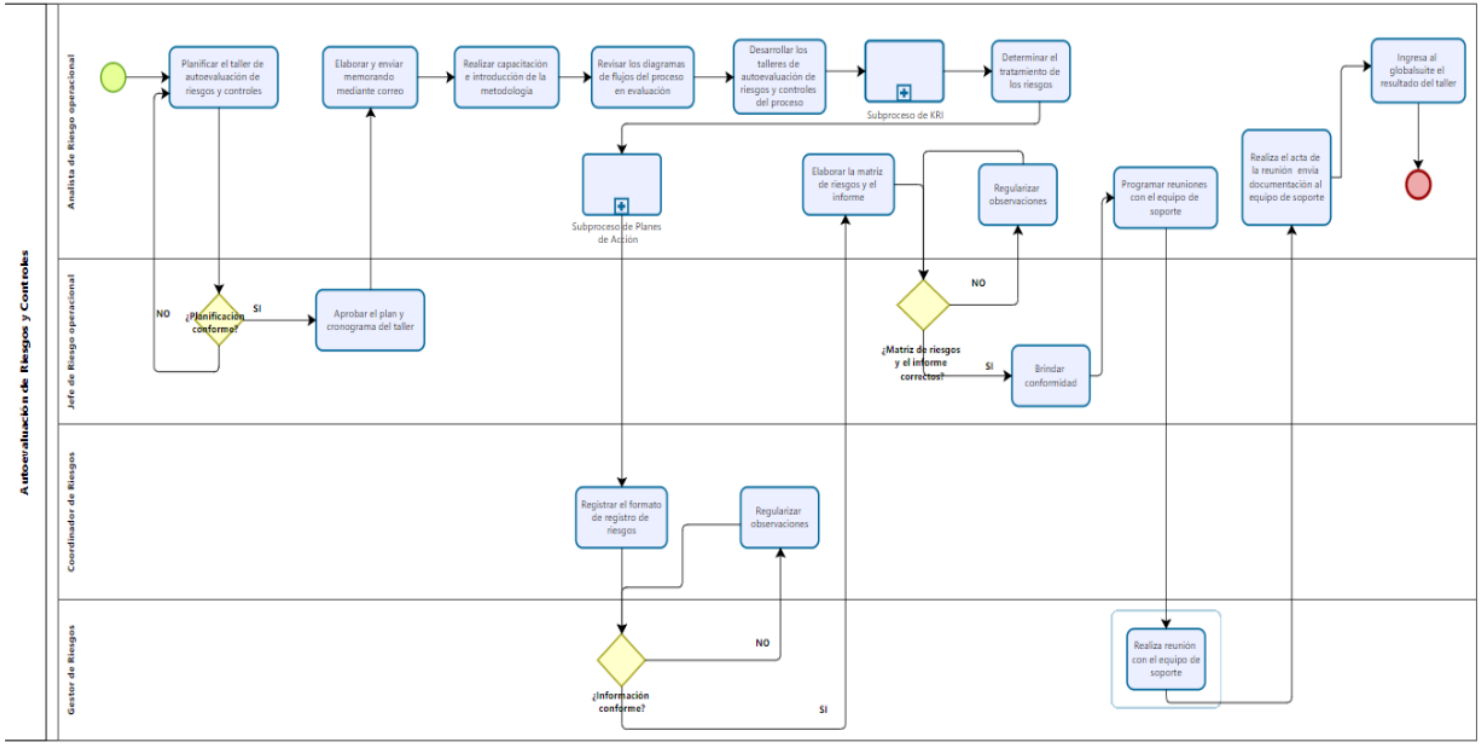
- Metodología de Indicadores Clave de Riesgos, son métricas que permiten realizar un seguimiento y monitoreo a los riesgos operacionales identificados en los talleres de autoevaluación de riesgos y controles. Los indicadores claves de riesgos cuentan con 02 parámetros (umbral mínimo y umbral máximo), estos valores son reportados de acuerdo con la periodicidad establecida y su estado podrían ser estable, revisión y alerta.

- Metodología de Planes de Acción, la cual consiste en establecer y monitorear las actividades y/o acciones que se implementaran para mitigar los riesgos operacionales identificados en un periodo de tiempo establecido. Cabe precisar que cuando un plan de acción se implementa se convierte en un control del riesgo evaluado.

Metodología de Autoevaluación de Riesgos y Controles

En la figura 11, se puede observar el diagrama de flujo que utiliza el equipo del Departamento de Riesgo de Operación y Tecnología para ejecutar la metodología de autoevaluación de riesgos y controles en coordinación con los usuarios involucrados. Asimismo, cabe precisar que también se realizó una revisión a la base de eventos o incidencias de riesgo operacional y a la base de datos de eventos de pérdida donde se identificó que se presentaron eventos.

Figura 11 *Diagrama de flujo "Autoevaluación de Riesgos y Controles"*



Fuente: Elaboración propia. Adaptado de la "DGP de Riesgo Operacional", por la entidad financiera. (2019)

N°	Responsable	Descripción de la actividad
1	-Analista de Riesgo Operacional	**Elaborar y presentar el Plan del Taller de Autoevaluación de Riesgos y Controles** 1. Elabora el plan y cronograma del Taller de Autoevaluación de Riesgos y Controles. 2. Presenta el plan y cronograma al Jefe de Riesgo Operacional.
2	- Jefe de Riesgo Operacional	**¿El plan y cronograma del taller está conforme?** **NO** **Hacia 03:** Solicita regularizar las observaciones **SÍ** **Hacia 04:** Comunica a los analistas la aprobación del plan y del cronograma.
3	- Analista de Riesgo Operacional	**Regularizar observaciones** 1. Regularizar observaciones. 2. Una vez subsanada la documentación, envía de nuevo la planificación al Jefe de Riesgo Operacional para su revisión.
4	- Jefe de Riesgo Operacional	**Comunicar la aprobación del plan y cronograma** del **Taller de Autoevaluación de Riesgos y Controles** 1. Comunica mediante correo electrónico la aprobación del plan y cronograma al analista de riesgo operacional responsable.
5	- Analista de Riesgo Operacional	**Elaborar y enviar el memorando del Taller a los involucrados del proceso** 1. Revisa de forma rápida los diagramas de flujos del proceso que se evaluará. 2. Identifica a las áreas involucradas en el proceso y designa el gestor y coordinador de riesgos responsable. 3. Elabora el memorando y envía mediante correo electrónico a los involucrados del proceso, gestor y coordinador de riesgos que participará en el taller con copia a las gerencias correspondiente informando el inicio y las actividades que se realizarán en los talleres.
6	- Analista de Riesgo Operacional	**Realizar capacitación de las metodologías de riesgo operacional a los involucrados** 1. Programa reunión y realiza capacitación de las metodologías de riesgo operacional, entre ellas la de Autoevaluación de Riesgos y Controles, Planes de Acción e Indicadores Clave de Riesgos.
7	- Analista de Riesgo Operacional	**Revisar los diagramas de los flujos del proceso** 1. Revisa y comprende los diagramas de flujos del proceso que se evaluará. 2. Revisa el mapa y la matriz de riesgos, donde identifica los riesgos detectados anteriormente. 3. En caso de encontrar algún riesgo anterior, informa los riesgos a reevaluar al gestor y coordinador de riesgos. 4. Coordina con el gestor y coordinador de riesgos responsable la disponibilidad de horario para el desarrollo del taller.

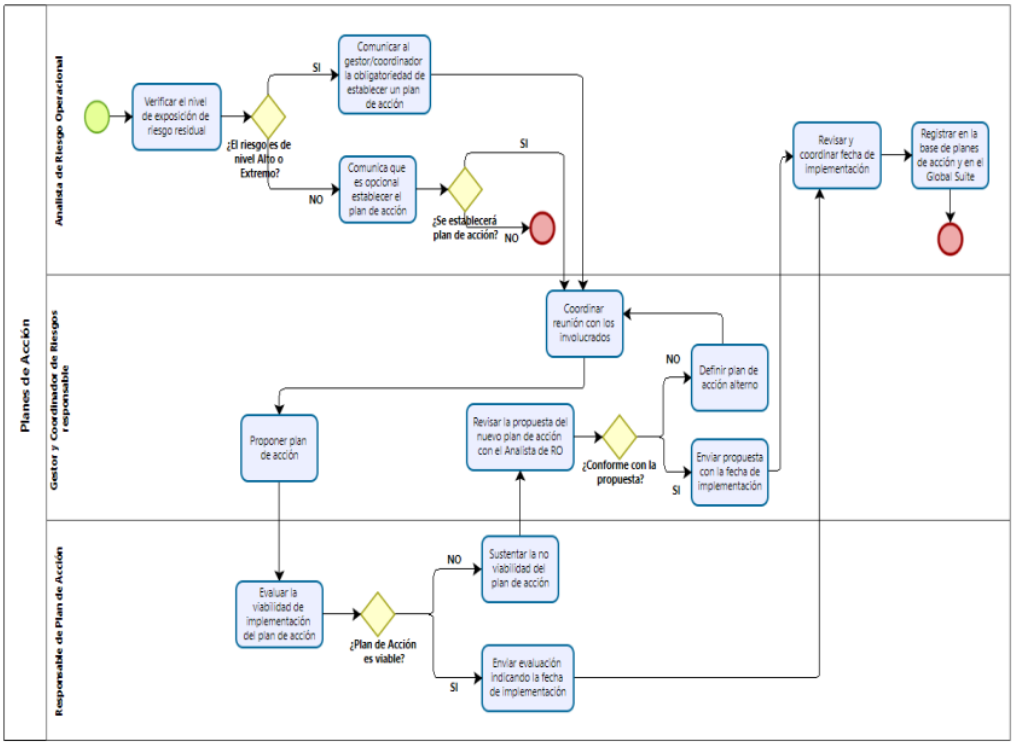
N°	Responsable	Descripción de la actividad
8	- Analista de Riesgo Operacional	**Desarrollar del Taller de Autoevaluación de Riesgos y Controles** 1. Se identifican y/o reevalúan los riesgos detectados en el proceso analizado con la participación de los involucrados. 2. Se identifican los controles asociados a los riesgos detectados del proceso analizado. 3. Se realiza la evaluación de los riesgos en función a la frecuencia y el impacto. Asimismo, se realiza la evaluación de los controles de acuerdo a lo establecido en la normativa.
9		**Subproceso: Indicadores Clave de Riesgos (KRI)**
10	- Analista de Riesgo Operacional	**Determina el tratamiento de los riesgos** 1. Se realiza la priorización de los riesgos residuales y se determina el tratamiento de los riesgos.
11		**Subproceso: Planes de Acción (PDA)**
12	- Coordinador de Riesgos responsable	**Registrar el formato de registro de riesgo** 1. En coordinación con los involucrados del taller, completa el formato de registro del riesgo operacional. 2. Envía el formato con la información correspondiente al Gestor de Riesgos para la validación correspondiente.
13	- Gestor de Riesgo responsable	**Recibe y revisa formato de registro de riesgo** 1. Recibe el formato de registro de riesgos enviado por el Coordinador de Riesgos y revisa la información contenida.
14		**¿Información conforme?** **NO** **Hacia 15:** Solicita regularizar observaciones **SÍ** **Hacia 16:** Elaborar Matriz de Riesgo y el Informe del taller
15	- Coordinador de Riesgos responsable	**Regularizar observaciones** 1. Regulariza las observaciones. 2. Una vez subsanada la documentación, envía de nuevo el formato de riesgos al Gestor de Riesgos para su revisión.
16	- Analista de Riesgo Operacional	**Elaborar Matriz de Riesgos y el informe con los resultados del taller** 1. Elabora la matriz de riesgo con lo identificado en el taller de autoevaluación. 2. Elabora el informe con los resultados obtenidos del proceso evaluado para el Equipo de Soporte. 3. Envía al Jefe de Riesgo Operacional para la revisión.
17	- Jefe de Riesgo Operacional	**Revisa la Matriz de Riesgo y el informe** 1. Revisa el contenido de la matriz de riesgo y el informe del taller de autoevaluación de riesgos y controles del proceso evaluado. 2. Analiza resultado de evaluación de riesgos y controles.

N°	Responsable	Descripción de la actividad
18		**¿Conforme?** **NO** **Hacia 19:** Solicita regularizar observaciones. **SÍ** **Hacia 20:** Brinda conformidad
19	- Analista de Riesgo Operacional	**Regularizar observaciones** 1. Regularizar observaciones. 2. Una vez subsanada las observaciones, envía de nuevo la matriz y el informe de riesgos del taller al Jefe de Riesgo Operacional para su revisión.
20	- Jefe de Riesgo Operacional	**Brinda conformidad** 1. Envía mediante correo electrónico la conformidad de la documentación y presentación al Analista de Riesgo Operacional.
21	- Analista de Riesgo Operacional	**Programar reunión con el Equipo de Soporte** 1. Coordina la disponibilidad de horario y programa reunión con el Equipo de Soporte.
22	- Gestor y Coordinador de Riesgos responsable	**Realiza reunión con Equipo de Soporte** 1. Presenta al equipo de soporte lo trabajado en los talleres de Autoevaluación de Riesgos y Controles: - Riesgos identificados y/o reevaluados del proceso evaluado. - Evaluación de riesgos y controles. - Propuesta de Planes de Acción e Indicadores Clave de Riesgos (KRI) planteados. 2. En caso de tener alguna observación, se modifica con el Equipo de Soporte 3. Solicita la aprobación de todo lo presentado al Equipo de Soporte.
23	- Analista de Riesgo Operacional	**Realizar el acta de la reunión** 1. Realizar y enviar el acta de la reunión para la aprobación formal mediante el correo electrónico. Asimismo, se debe adjuntar la matriz de riesgos, el informe del taller y los formatos de registros de riesgos para las firmas correspondientes.
24	- Analista de Riesgo Operacional	**Ingresar la matriz de riesgos al Global Suite** 1. Ingresa al Global Suite el resultado de la matriz de riesgo del Taller de Autoevaluación de Riesgos y Controles del proceso evaluado. 2. Carga en el sistema los siguientes documentos: - Formatos de registro de riesgo operacional. - Informe del proceso evaluado. - Matriz de riesgos. - Acta de reunión del Equipo de Soporte. **Fin del procedimiento**

Metodología de Planes de Acción

En la siguiente figura 12, se puede observar el diagrama de flujo que utiliza el equipo del Departamento de Riesgo de Operación y Tecnología para ejecutar la metodología de planes de acción con los usuarios involucrados.

Figura 12 *Diagrama de flujo "Planes de Acción"*



Fuente: Elaboración propia. Adaptado de la "DGP de Riesgo Operacional", por la entidad financiera. (2019)

N°	Responsable	Descripción de la actividad
1	- Analista de Riesgo Operacional.	**Verifica el nivel de exposición de riesgo** 1. Verificar el nivel de exposición del riesgo residual a fin de determinar la necesidad de establecer planes de acción.
2	- Analista de Riesgo Operacional.	**¿El riesgo es Alto o Extremo?** **SÍ** **Hacia 03:** Comunicar que deben establecer un plan de acción. **NO** **Hacia 04:** Comunicar que establecer el plan de acción es opcional.

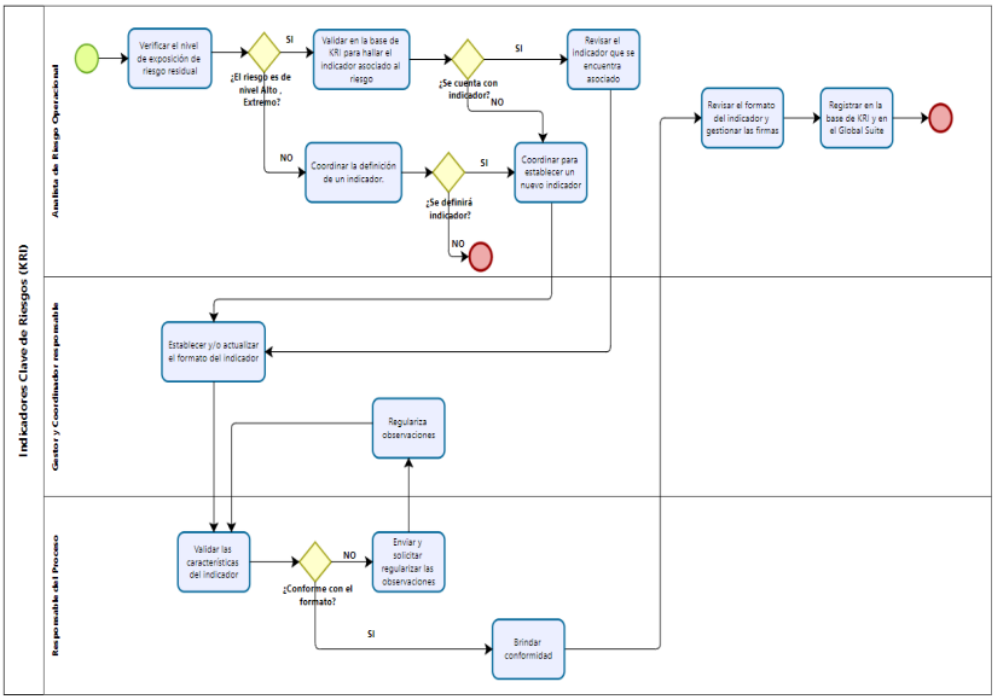
N°	Responsable	Descripción de la actividad
3	- Analista de Riesgo Operacional.	**Comunicar que se debe establecer un plan de acción** 1. Comunicar al gestor/coordinador de riesgos responsable que para los riesgos con nivel de exposición Extremo o Alto, la definición del Plan de Acción es obligatoria. **Continua con la actividad N° 6**
4	- Analista de Riesgo Operacional.	**Comunicar que establecer el plan de acción es opcional** 1. Comunicar al gestor/coordinador de riesgos responsable que para los riesgos con nivel de exposición Medio o Bajo la definición del Plan de Acción es opcional.
5	- Analista de Riesgo Operacional.	**¿Se establecerá plan de acción?** **NO** Fin del procedimiento. **SÍ** **Hacia 06:** Coordinar reunión para establecer un nuevo indicador
6	- Gestor y Coordinador de Riesgos responsable	**Coordinar para establecer un nuevo indicador** 1. Se coordina una reunión con los involucrados para establecer o proponer un Plan de Acción. 2. Programa reunión de acuerdo a la disponibilidad de horario de los involucrados.
7	- Gestor y Coordinador de Riesgos responsable	**Proponer plan de acción** 1. En la reunión con los involucrados se propone el nuevo plan de acción que ayudará a mitigar la exposición del riesgo. 2. Solicita al responsable del plan de acción que evalue la viabilidad de la implementación.
8	- Responsable de la implementación del PA.	**Evaluar viabilidad de implementación del plan de acción** 1. Evalúa viabilidad de implementación del Plan de Acción propuesto, determinando fecha de implementación e informe de inversión, si fuera el caso.
9	- Responsable de la implementación del PA.	**¿Plan de Acción es viable?** **SÍ** **Hacia 10:** Envía evaluación mediante correo electrónico. **NO** **Hacia 11:** Sustenta la no viabilidad del Plan de Acción
10	- Responsable de la implementación del PA.	**Envía evaluación de viabilidad** 1. Envía mediante correo la evaluación del Plan de Acción al Analista de Riesgo Operacional indicando fechas de implementación. - *Los riesgos con nivel de exposición residual Extremo, el plazo máximo de implementación es de 06 meses.* - *Los riesgos con nivel de exposición residual Alto, el plazo máximo de implementación es de 09 meses.* **Continua con la actividad N° 16**

N°	Responsable	Descripción de la actividad
11	- Responsable de la implementación del PA.	**Sustenta la no viabilidad del Plan de Acción** 1. Sustenta la no viabilidad del Plan de Acción indicando los motivos, y, de ser el caso, propone un nuevo Plan de Acción.
12	- Gestor y Coordinador de Riesgos responsable	**Revisar la propuesta del nuevo plan de acción** 1. Recibe respuesta del responsable de la implementación del plan de acción indicando que no es viable. Asimismo envía la propuesta del nuevo Plan de Acción para que sea revisada con el Analista de Riesgo Operacional.
13	- Gestor y Coordinador de Riesgos responsable	**¿Propuesta del nuevo plan de acción es conforme?** **NO** **Hacia 14:** Definir un Plan de Acción alterno **SÍ** **Hacia 15:** Enviar propuesta con la fecha de implementación
14	- Gestor y Coordinador de Riesgos responsable	**Definir un plan de acción alterno** 1. Coordina con el responsable de implementación del plan de acción para definir un plan de acción alterno. **Continua con la actividad N° 6**
15	- Gestor y Coordinador de Riesgos responsable	**Enviar propuesta con la fecha de implementación** 1. Enviar propuesta del plan de acción con la fecha de implementación. - *Los riesgos con nivel de exposición residual Extremo, el plazo máximo de implementación es de 06 meses.* - *Los riesgos con nivel de exposición residual Alto, el plazo máximo de implementación es de 09 meses.*
16	- Analista de Riesgo Operacional.	**Revisar y coordinar la fecha de implementación** 1. Revisar que las fechas de implementación cumplan con el plazo indicado de 6 y 9 meses según el nivel de riesgo.
17	- Analista de Riesgo Operacional.	**Registrar la información en la base de planes de acción y en el Global Suite.** 1. Registra el Plan de Acción en la base de planes de acción y lo ingresa en el sistema del global suite. **Fin del procedimiento**

Metodología de Indicadores Clave de Riesgos

En la figura 13, se puede observar el diagrama de flujo que utiliza el equipo del Departamento de Riesgo de Operación y Tecnología para ejecutar la metodología de indicadores clave de riesgos. Cabe precisar que se detallará el proceso de definición y/o registro del indicador y el seguimiento correspondiente.

Figura 13 *Diagrama de flujo "Indicadores Clave de Riesgos"*



Fuente: Elaboración propia. Adaptado de la "DGP de Riesgo Operacional", por la entidad financiera. (2019)

N°	Responsable	Descripción de la actividad
1	- Analista de Riesgo Operacional.	**Verificar el nivel de exposición de riesgo residual** 1. Verificar el nivel de exposición del riesgo residual a fin de determinar la necesidad de establecer indicadores clave de riesgo.
2	- Analista de Riesgo Operacional.	**¿El riesgo es Alto o Extremo?** **NO** **Hacia 03:** Coordinar la definición de un indicador **SÍ** **Hacia 05:** Valida en la base de KRI
3	- Analista de Riesgo Operacional.	**Coordinar si se determina la definición de un indicador.** 1. Coordinar con el gestor / coordinador de riesgos si se determina la necesidad de definir o establecer un indicador. *(*) Cabe precisar que los riesgos con nivel de exposición residual medio o bajo, la definición de un KRI es opcional.*
4		**¿Se definirá indicador?**

N°	Responsable	Descripción de la actividad
	- Analista de Riesgo Operacional.	**NO** Fin del procedimiento. **SÍ** **Hacia 07:** Coordina para establecer un nuevo indicador
5	- Analista de Riesgo Operacional.	**Validar en la base de KRI** 1. Valida en la base de Indicadores Claves de Riesgos e identifica que no haya un indicador asociado al riesgo, en caso exista un indicador, se deberá reevaluar y/o revisar el KRI.
6	- Analista de Riesgo Operacional.	**¿Se cuenta con indicador relacionado en la base de KRI?** **NO** **Hacia 07:** Coordina para establecer un nuevo indicador **SÍ** **Hacia 08:** Revisar el indicador que se encuentra asociado.
7	- Analista de Riesgo Operacional.	**Coordina para establecer un nuevo indicador** 1. Coordinar con el gestor / coordinador de riesgos para establecer o definir un nuevo indicador, este debe estar asociado al riesgo. ***Continua con la actividad N° 9***
8	- Analista de Riesgo Operacional.	**Revisar el indicador que se encuentra asociado.** 1. Busca y revisa el formato de registro del indicador y lo envía al gestor / coordinador de riesgos. para establecer o definir un nuevo indicador.
9	- Gestor y Coordinador de Riesgos responsable	**Elaborar o actualizar el formato de registro del indicador** 1. Elabora/actualiza el formato de registro del Indicador Clave de Riesgo (KRI) completando el formato. Cabe mencionar que esto lo envía mediante correo electrónico al responsable del proceso.
10	- Responsable del proceso	**Validar las características del indicador** 1. Revisa y valida que todos los campos del formato del Indicador Clave de Riesgo se encuentren conforme a lo coordinado. *(*) Valida las características del indicador, tales como la descripción, la fórmula de cálculo, los umbrales establecidos, fuente de información, la frecuencia de reporte y el sustento.*
11	- Responsable del proceso	**¿Formato de registro de indicador conforme?** **NO** **Hacia 12:** Envía las observaciones **SÍ** **Hacia 13:** Envía la conformidad del registro mediante correo electrónico.
12	- Responsable del proceso	**Remite observaciones** 1. Envía mediante correo electrónico al gestor / coordinador responsable las observaciones detectadas en el formato de registro del Indicador Clave de Riesgo (KRI) para la regularización correspondiente.

N°	Responsable	Descripción de la actividad
13	- Responsable del proceso	**Brindar conformidad** 1. Envía mediante correo electrónico la conformidad sobre el formato de registro del indicador junto con la conformidad del gestor/coordinador de riesgos.
14	- Analista de Riesgo Operacional.	**Revisa el formato del Indicador Clave de Riesgo y gestiona las firmas** 1. Revisa que todos los campos del formato de registro del Indicador Clave de Riesgo se encuentren completos y conformes. 2. Coordina y gestiona las firmas correspondientes en el formato de registro del indicador (responsable del proceso, gestor y coordinador de riesgos, responsable de fuente de información y analista de riesgo operacional)
15	- Analista de Riesgo Operacional	**Registra el Indicador en la Base de KRI y en el Global Suite** 1. Verifica las firmas y archiva el formato del registro de indicador clave de riesgos. Asimismo, escanea el formato y lo guarda en el file server. 2. Registra en la Base de KRI y en el sistema del Global Suite. **Fin del procedimiento**

4.3.2. Identificación y Evaluación de Riesgos Operacionales

La autoevaluación de riesgos y controles de los procesos de Gestión de Tecnología es necesario para gestionar y analizar los riesgos mejorando los controles internos y por ende mejorar la calidad del proceso. Asimismo, se previene futuros riesgos operacionales que podrían ocasionar pérdidas al banco.

Entendimiento de proceso

En esta primera etapa, se realizó el plan de trabajo que consistió en contar con un cronograma de actividades de la autoevaluación de riesgos y controles de los tres procesos de Gestión de Tecnología.

En la tabla 5, se podrá observar el cronograma de actividades que se estableció para la autoevaluación de riesgos y controles del proceso.

Tabla 5 *Cronograma de actividades*

N°	Actividades		Inicio	Fin	Nov-19				Dic-19				Ene-20			
					1	2	3	4	1	2	3	4	1	2	3	4
1	Capacitación Presencial y virtual a los involucrados		4/11/2019	10/11/2019												
2	Taller de Riesgos - Identificación y evaluación de riesgos	Gestión de Requerimientos TI	11/11/2019	17/11/2019												
		Gestión de Cambios TI	18/11/2019	24/11/2019												
		Gestión de Servicios TI	25/11/2019	1/12/2019												
3	Taller de Riesgos - Evaluación de controles	Gestión de Requerimientos TI	2/12/2019	8/12/2019												
		Gestión de Cambios TI	9/12/2019	15/12/2019												
		Gestión de Servicios TI	16/12/2019	22/12/2019												
4	Taller de Riesgos - Definición de Planes de Acción y los Indicadores Clave de Riesgos		23/12/2019	1/01/2020												
5	Elaboración de Matriz de Riesgo y presentación		2/01/2020	5/01/2020												
6	Presentación de la autoevaluación de riesgo al Equipo de Soporte		6/01/2020	8/01/2020												
7	Elaboración de Acta del Equipo de Soporte		9/01/2020	12/01/2020												
8	Emisión de Informe de la autoevaluación de riesgo del proceso		13/01/2019	19/01/2020												

Nota: Se muestra las actividades que se realizarán en los talleres de autoevaluación de riesgos y controles. Elaboración propia.

Asimismo, se revisó los diagramas de flujos de actividades de los diferentes procesos que se encuentran en los anexos con el objetivo de comprender y entender dichos procesos e identificar a los usuarios involucrados.

A continuación, se podrá observar los usuarios involucrados en los procesos:

Tabla 6 *Participantes del taller de autoevaluación de riesgos y controles*

DIVISIÓN	CARGO
Operaciones y Tecnologías	Jefe de Dpto. Gestión de Servicios de T.I.
	Jefe de Sección de Infraestructura y Control de Calidad
	Responsable TDP
	Jefe de Dpto. Desarrollo de Sistemas

DIVISIÓN	CARGO
	Jefe de Sección de Planificación y Control
	Jefe de Proyecto de TI
	Analista de Control de Calidad
	Analista de Sistemas
	Analista de Gestión de Servicios T.I.
	Asistente de Planificación y Control
	Jefe de Unidad Atención de Reclamos
Innovación y Estrategia del Cliente	Líder de Gestión de Procesos
	Jefe de Sec. Desarrollo de Segmentos
Legal	Jefe de Sec. Asuntos Judiciales y Adm.
Riesgos	Jefe de Sec. Gestión de Riesgo de Fraude
	Jefe de Sec. Seguridad de La Información
Usuario (Agencia)	Jefe de Servicios - Oficina Principal

Nota: Elaboración propia

Por otro lado, se muestra la estimación del presupuesto que se requirió para el desarrollo de la mejora del proceso de gestión de tecnología aplicando las metodologías de riesgo operacional. En la siguiente tabla 7, se puede observar el detalle del presupuesto.

Tabla 7 *Presupuesto*

CONCEPTO			Mes 1	Mes 2	Mes 3	Total
Gestión de Recursos Humanos			17,050.00	17,050.00	17,050.00	51,150.00
Analista de Riesgo Operacional	60%	4,000.00	2,400.00	2,400.00	2,400.00	7,200.00
Personal asistente a los talleres						
Jefe de Dpto. Gestión de Servicios de T.I.	15%	7,500.00	1,125.00	1,125.00	1,125.00	3,375.00
Jefe de Sección de Infraestructura y Control de Calidad	30%	5,000.00	1,500.00	1,500.00	1,500.00	4,500.00
Responsable TDP	20%	5,000.00	1,000.00	1,000.00	1,000.00	3,000.00
Jefe de Dpto. Desarrollo de Sistemas	20%	8,000.00	1,600.00	1,600.00	1,600.00	4,800.00
Jefe de Sección de Planificación y Control	30%	5,500.00	1,650.00	1,650.00	1,650.00	4,950.00
Jefe de Proyecto de TI	20%	5,000.00	1,000.00	1,000.00	1,000.00	3,000.00
Analista de Control de Calidad	30%	3,000.00	900.00	900.00	900.00	2,700.00
Analista de Sistemas	20%	2,500.00	500.00	500.00	500.00	1,500.00
Analista de Gestión de Servicios T.I.	40%	2,500.00	1,000.00	1,000.00	1,000.00	3,000.00

CONCEPTO			Mes 1	Mes 2	Mes 3	Total
Asistente de Planificación y Control	30%	2,000.00	600.00	600.00	600.00	1,800.00
Jefe de Unidad Atención de Reclamos	10%	4,000.00	400.00	400.00	400.00	1,200.00
Líder de Gestión de Procesos	25%	3,500.00	875.00	875.00	875.00	2,625.00
Jefe de Sec. Desarrollo de Segmentos	5%	4,000.00	200.00	200.00	200.00	600.00
Jefe de Sec. Asuntos Judiciales y Adm.	5%	5,000.00	250.00	250.00	250.00	750.00
Jefe de Sec. Gestión de Riesgo de Fraude	10%	5,000.00	500.00	500.00	500.00	1,500.00
Jefe de Sec. Seguridad de La Información	15%	7,000.00	1,050.00	1,050.00	1,050.00	3,150.00
Jefe de Servicios - Oficina Principal	20%	2,500.00	500.00	500.00	500.00	1,500.00
Gastos de Equipos y Artículos de Oficina			2,000.00	2,000.00	2,000.00	6,000.00
Pérdida mensual estimada en base a las pérdidas (Agosto 2018 hasta Julio 2019)			25,821.10	25,821.10	25,821.10	77,463.31
Total Presupuesto			**44,871.10**	**44,871.10**	**44,871.10**	134,613.31

Nota: La tabla contiene el detalle del presupuesto.

Identificación de Riesgos

Esta etapa consistió en identificar los riesgos asociados a las actividades vinculadas al proceso que se está evaluando, también se realizó la evaluación del riesgo operacional inherente al proceso. Las herramientas que fueron utilizadas para identificar los riegos incluyen el juicio basado en la experiencia y las entrevistas a profundidad.

Luego de realizar el análisis y entendimiento de los flujos de cada proceso, se llevó a cabo los talleres con los involucrados mencionados anteriormente donde se identificaron los siguientes riesgos según cada proceso evaluado:

Tabla 8 *Riesgos del proceso de Gestión de Requerimientos TI*

Proceso	N° Riesgo	Descripción del Riesgo	Factor de Riesgo	Causas	Consecuencias
Gestión de Requerimientos de TI	**R1**	Posibilidad de pérdida económica por no identificar de forma correcta a los usuarios en la	Procesos Internos	1. Falta de mecanismos para la identificación de usuario final por parte de Mesa de Ayuda.	1.Suplantación de Identidad (Fraude Interno) 2. Fuga de Información

Proceso	N° Riesgo	Descripción del Riesgo	Factor de Riesgo	Causas	Consecuencias
		atención de solicitudes.			
Gestión de Requerimientos de TI	**R2**	Posibilidad de pérdida económica debido a una inadecuada y/o inoportuna atención de incidentes / requerimientos en los plazos establecidos.	Personal	1. Inadecuada priorización y análisis de la atención de los tickets. 2. Falta de conocimiento de los procesos y sistemas involucrados. 3. Recepción de documentación incompleta y/o incorrecta. 4. Inadecuada elaboración del documento solución. 5. Falta de seguimiento en la atención de incidencias y requerimientos.	1. Reprogramaciones de requerimientos. 2. Multas y/o sanciones del ente regulador. 3. Acumulación de solicitudes 4. Incremento del costo del requerimiento.
Gestión de Requerimientos de TI	**R3**	Posibilidad de pérdida económica debido a no contar con un adecuado control de las solicitudes de requerimientos /incidentes atendidos por el proveedor.	Procesos Internos	1. Inadecuado ingreso de solicitudes de requerimientos e incidentes (incidentes independientes siendo incidencias masivas). 2. Inadecuada categorización de los requerimientos e incidentes.	1. Exceso de costo en el servicio del proveedor de TI.

Nota: La tabla contiene el riesgo identificado, factor de riesgo, causas y consecuencias que origina el riesgo.

Tabla 9 *Riesgos del proceso de Gestión de Cambios TI*

Proceso	N° Riesgo	Descripción del Riesgo	Factor de Riesgo	Causas	Consecuencias
Gestión de Cambios de TI.	**R4**	Posibilidad de pérdida económica por un inadecuado análisis y diseño de pruebas en control de calidad.	Personal	1. Falta de personal capacitado 2. Pruebas de calidad insuficientes.	1. Cambios puestos en producción con errores o no son los esperados por el usuario. 2. Retrabajo al realizar nuevamente el desarrollo del software. 3. Incumplimiento de plazos.
Gestión de Cambios de TI.	**R5**	Posibilidad de pérdida económica debido a indisponibilidad de los servicios.	Procesos Internos	1. Inadecuado procedimiento para analizar y dimensionar el impacto de los pases a realizar. 2. Falta de personal técnico para priorizar los cambios requeridos. 3. Error humano 4. No cumplimientos de los procedimientos establecidos	1. Multa del ente regulador por incumplimiento de normativa vigente. 2. Multa del ente regulador debido a reclamos de clientes por indisponibilidad de los servicios. 3. Riesgo Reputacional
Gestión de Cambios de TI.	**R6**	Posibilidad de pérdida económica por errores en las operaciones efectuadas en el sistema debido a una administración inadecuada de fuentes.	Procesos Internos	1. Inadecuado versionamiento del código fuente. 2. Problemas en la administración de repositorio de custodia de fuentes. 3. Falta de personal técnico.	1. Multa del ente regulador por reclamos de los clientes. 2. Reaparición de incidencias /Comportamiento anómalo del aplicativo. 3. Indisponibilidad de los servicios para la atención al público.

Nota: La tabla contiene el riesgo identificado, factor de riesgo, causas y consecuencias que origina el riesgo.

Tabla 10 *Riesgos del proceso de Gestión de Servicios TI*

Proceso	N° Riesgo	Descripción del Riesgo	Factor de Riesgo	Causas	Consecuencias
Gestión de Servicios TI	**R7**	Posibilidad de pérdida económica por daño y/o pérdida de los backup's de información del banco afectando la disponibilidad e integridad de la información.	Procesos Internos	1. Deterioro de los medios magnéticos. 2. Falta de verificación por parte de las áreas de control ante el borrado y destrucción de los medios de almacenamiento (se corrobore que la información ya este almacenada en otro backup, que la información no se pueda reconstruir) 3. Falta de revisión y verificación de los inventarios de control de medios magnéticos.	1. Multas y/o sanciones 2. Pérdida de Información
Gestión de Servicios TI	**R8**	Posibilidad de pérdida económica por divergencia de responsabilidades de los servicios ofrecidos por el proveedor.	Procesos Internos	1.Desconocimiento del alcance del contrato. 2. Discrepancias en las responsabilidades por parte del proveedor y del banco.	1.Falta de ejecución de actividades
Gestión de Servicios TI	**R9**	Posibilidad de pérdida económica por la indisponibilidad de servicios TI debido a que no se tiene establecido los horarios	Procesos Internos	1. No se tiene actualizado los horarios de los servicios TI (solo consideraron siaf y fitbank y se debe incluir todos los servicios incluidos los 24/7). 2. No se brinda o comparte los horarios tipificados de los servicios TI con el proveedor.	1. Indisponibilidad de servicios TI 2. Multa y/o sanciones 3. Reclamo de Clientes
Gestión de Servicios TI	**R10**	Posibilidad de pérdida económica por no realizar seguimiento a los activos tecnológicos (PCs, Laptops, etc.).	Personal	1. Inadecuado seguimiento y/o supervisión de los activos tecnológicos. 2. Inventario de activos tecnológicos desactualizado.	1. Costo de reposición de activos tecnológicos. 2. Pérdida de los activos tecnológicos

Proceso	N° Riesgo	Descripción del Riesgo	Factor de Riesgo	Causas	Consecuencias
				3. No se encuentra actualizado el proceso.	

Nota: La tabla contiene el riesgo identificado, factor de riesgo, causas y consecuencias que origina el riesgo.

Evaluación de Riesgos Inherentes

Asimismo, en el taller y según la metodología de autoevaluación de riesgos, se procedió a cuantificar y evaluar el riesgo inherente. Para la cuantificación de los riesgos operacionales, se utilizaron 02 criterios los cuales permiten establecer la magnitud de la materialización del riesgo siendo el "Impacto" y la probabilidad de ocurrencia de que el riesgo se materialice denominado "Frecuencia". Cada criterio cuenta con 05 escalas de valorización o rangos para permitir un entendimiento del impacto causado por la materialización de un riesgo operacional, las cuales se muestran en los siguientes cuadros.

Tabla 11 *Escalas de valorización de Frecuencia.*

Nivel de Frecuencia	Valor	En un marco de tiempo	En el grado de ocurrencia
Casi Cierto	5	El riesgo se podría materializar en forma mensual	Mensual
Muy Probable	4	El riesgo se podría materializar en forma semestral	Semestral
Moderado	3	El riesgo se podría materializar cada año	Anual
Improbable	2	El riesgo se podría materializar una vez cada dos (2) años	Una vez cada dos (2) años
Raro	1	El riesgo se podría materializar una vez cada cuatro (4) años	Una vez cada cuatro (4) años

Nota: Adaptado del "MPP de Riesgo Operacional", por la entidad financiera. (2020)

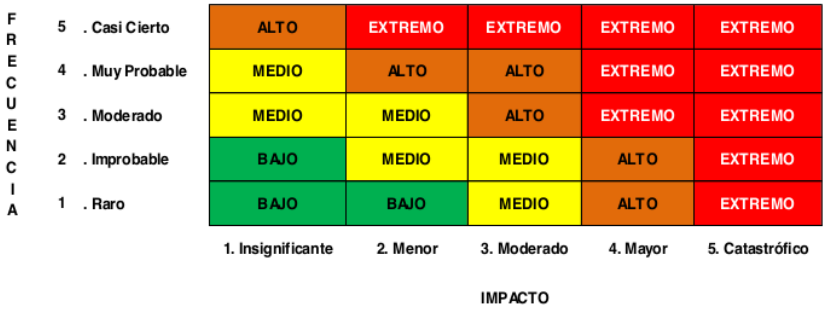
Tabla 12 *Escalas de valorización de Impacto.*

Nivel de Impacto	Valor	En el impacto financiero
Catastrófico	5	La pérdida financiera amenaza la salud del Banco (más de S/ 535,672.13).
Mayor	4	La pérdida financiera tiene un impacto material en el logro de objetivos financieros (más de S/ 178,557.38 y hasta S/ 535,672.13).
Moderado	3	La pérdida financiera tiene un impacto notable en el logro de objetivos financieros (más de S/ 89,278.69 y hasta S/ 178,557.38).
Menor	2	La pérdida financiera puede ser absorbida como un gasto operativo y tiene mínimo impacto en los objetivos financieros (más de S/ 35,711.48 y hasta S/ 89,278.69).
Insignificante	1	La pérdida financiera no impacta en el logro de objetivos financieros (hasta S/ 35,711.48)

Nota: Adaptado del "MPP de Riesgo Operacional", por la entidad financiera. (2020)

De acuerdo con la calificación obtenida en el nivel de frecuencia e impacto, se determinó la calificación del riesgo inherente pudiendo tomar cuatro valores (Bajo, Medio, Alto y Extremo), para ello se utiliza la matriz de apetito y límite de riesgo operacional.

Figura 14 *Matriz de Apetito y Límites al Riesgo Operacional*



Fuente: Intranet de la Entidad Financiera (2020)

A continuación, se muestra la calificación del riesgo inherente obtenida de los siguientes riesgos:

Tabla 13 *Calificación de riesgo inherente*

Proceso	N° Riesgo	Descripción del Riesgo	Frecuencia	Impacto	Nivel de Riesgo Inherente
Gestión de Requerimientos de TI	**R1**	Posibilidad de pérdida económica por no identificar de forma correcta a los usuarios en la atención de solicitudes.	**4**	**2**	**ALTO**
Gestión de Requerimientos de TI	**R2**	Posibilidad de pérdida económica debido a una inadecuada y/o inoportuna atención de incidentes / requerimientos en los plazos establecidos.	5	1	**ALTO**
Gestión de Requerimientos de TI	**R3**	Posibilidad de pérdida económica debido a no contar con un adecuado control de las solicitudes de requerimientos /incidentes atendidos por el proveedor.	4	3	**ALTO**
Gestión de Cambios de TI.	**R4**	Posibilidad de pérdida económica por un inadecuado análisis y diseño de pruebas en control de calidad.	4	1	**MEDIO**
Gestión de Cambios de TI.	**R5**	Posibilidad de pérdida económica debido a indisponibilidad de los servicios.	5	1	**ALTO**
Gestión de Cambios de TI.	**R6**	Posibilidad de pérdida económica por errores en las operaciones efectuadas en el sistema debido a una administración inadecuada de fuentes.	4	2	**ALTO**
Gestión de Servicios TI	**R7**	Posibilidad de pérdida económica por daño y/o pérdida de los backup's de información del banco afectando la disponibilidad e	3	4	**EXTREMO**

Proceso	N° Riesgo	Descripción del Riesgo	Frecuencia	Impacto	Nivel de Riesgo Inherente
		integridad de la información.			
Gestión de Servicios TI	**R8**	Posibilidad de pérdida económica por divergencia de responsabilidades de los servicios ofrecidos por el proveedor.	3	3	**ALTO**
Gestión de Servicios TI	**R9**	Posibilidad de pérdida económica por la indisponibilidad de servicios TI debido a que no se tiene establecido los horarios	3	3	**ALTO**
Gestión de Servicios TI	**R10**	Posibilidad de pérdida económica por no realizar seguimiento a los activos tecnológicos (PCs, Laptops, etc.).	4	2	**ALTO**

Nota: La tabla contiene el riesgo identificado por cada proceso, con el valor de la frecuencia e impacto y el nivel de riesgo inherente.

4.3.4. Identificación y Evaluación de los Controles del proceso

Se realizó la identificación y evaluación de los controles asociados a los riesgos inherentes identificados, en el cual los usuarios participantes o involucrados en el taller identifican los controles actuales que se manejan para mitigar la exposición al riesgo operacional del proceso. Los controles se encuentran clasificados en dos categorías: Preventivos y Detectivos.

Una vez identificados los controles, se procede a calificar el grupo de controles existentes asociados al riesgo, partiendo de la calificación individual de los mismos, considerando lo siguiente:

- Para determinar la calificación del control se utilizará la información del testeo de controles efectuado por Auditoría Interna, como resultado de sus revisiones,

aplicando una metodología de muestreo y dando como resultado tres valores: El control es Fuerte, Moderado o Débil.

- Para los casos de controles que no se cuente con información del testeo de controles se utilizará la información proporcionada por los usuarios en base al juicio experto, para la calificación de ello se utilizan dos variables: Diseño y Ejecución:
    - Diseño del control: se refiere si el control está bien definido a nivel teórico, es decir, si tal cual ha sido planteado y documentado logra mitigar la parte del riesgo para lo cual fue concebido. En la tabla 13, se definen las tres variables a tomar en cuenta para la calificación del Diseño del Control, cuyo promedio de los puntajes asignados será la calificación del diseño.

Tabla 14 *Variables de la calificación del diseño del control*

Variable del Diseño	Puntaje
Definición/ Documentación	
El control no se encuentra documentado.	1
El control se encuentra documentado, pero no actualizado.	5
El control se encuentra documentado y actualizado.	10
Objetivo	
El control mitiga el riesgo de forma temporal.	1
El control mitiga el riesgo parcialmente.	5
El control mitiga el riesgo efectivamente.	10
Automatización	
Control manal y debería ser automatizado.	1
Control combinado (manual - automatizado)	5
Control Automatizado / Control Manual	10

Nota: Adaptado del "MPP de Riesgo Operacional", por la entidad financiera. (2020)

- Ejecución del control: se refiere a que, si el control se realiza con la debida frecuencia y el adecuado cuidado, los puntajes asignados son los siguientes.

Tabla 15 *Variables de la calificación de ejecución del control*

Niveles	Descripción	Calificación
Débil	Nivel de Cumplimiento entre 0% a 74%	1
Moderado	Nivel de Cumplimiento entre 75% a 89%	5
Fuerte	Nivel de Cumplimiento entre 90% a 100%	10

Nota: Adaptado del "MPP de Riesgo Operacional", por la entidad financiera. (2020)

Según la calificación obtenida en el diseño y ejecución del control evaluado, se obtiene la calificación total del control.

Tabla 16 *Calificación del control según el diseño y ejecución*

Nivel de Diseño	Nivel de Ejecución	Calificación del Control
Débil	Fuerte, Moderado o Débil	Débil
Fuerte, Moderado o Débil	Débil	Débil
Moderado	Fuerte	Fuerte
Fuerte	Moderado	Moderado
Fuerte	Fuerte	Fuerte
Moderado	Moderado	Moderado

Nota: Adaptado del "MPP de Riesgo Operacional", por la entidad financiera. (2020)

Luego de haber realizado la calificación individual de los controles, se califica al grupo de controles, la cual será equivalente a la mayor calificación individual del control que conforma el grupo.

A continuación, se muestra los controles por cada riesgo identificado:

Tabla 17 *Identificación y calificación del control por cada riesgo detectado*

Identificación		Identificación			Efectividad		Calificación del Control							
							Diseño				Ejecución		Calificación del Control	Calificación del Grupo de Controles
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización					
R1	Posibilidad de pérdida económica por no identificar de forma correcta a los usuarios en la atención de solicitudes.	C1	Cada vez que se solicite la atención de una solicitud, el personal de Mesa de Ayuda solicita código de empleador o DNI del usuario final para verificar la autenticación.	Preventivo	X		El control no se encuentra documentado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado
		C2	Se ha habilitado a los Gerentes de Agencias la opción de desbloqueo de cuentas de los colaboradores de su equipo, estos usuarios no requieren llamar a Mesa de Ayuda.	Preventivo	X		El control no se encuentra documentado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	

Identificación		Identificación			Efectividad		Calificación del Control							
							Diseño				Ejecución			
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización				Calificación del Control	Calificación del Grupo de Controles
R2	Posibilidad de pérdida económica debido a una inadecuada y/o inoportuna atención de incidentes / requerimientos en los plazos establecidos.	C1	Cada vez que el usuario realiza una solicitud, el personal de Mesa de Ayuda analiza y realiza la priorización del ticket en base al impacto y urgencia (Prioridad crítica, Alta, Media y Baja) cumpliendo con los tiempos de la normativa.	Preventivo	X		El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado
		C2	De forma trimestral, se realiza la capacitación al personal de Mesa de Ayuda respecto a la priorización de los requerimientos y los documentos o sustentos que se debe solicitar según corresponda.	Preventivo	X		El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 90% a 100%	10	Fuerte	
		C3	El Analista de Sistemas evalúa el alcance, tiempo, recursos y así determina la solución y atención del requerimiento TI, en este último caso es	Preventivo	X		El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	

Identificación		Identificación			Efectividad		Calificación del Control							
							Diseño				Ejecución		Calificación del Control	Calificación del Grupo de Controles
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización					
			coordinado con el Jefe de Proyectos de TI para su atención.											
		C4	Cada vez que la atención de un ticket se demora o retrasa, el usuario coordina con el Analista de Gestión de Servicios para el seguimiento de la atención al requerimiento o incidencia.	Detectivo	X		El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Manual y debería ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	
R3	Posibilidad de pérdida económica debido a no contar con un adecuado control de las solicitudes de requerimientos /incidentes atendidos por el proveedor.	C1	De forma semanal el Dpto. de Gestión de Servicios TI analiza las incidencias y requerimientos a fin de controlar el pago de la factura mensual proporcionada por el proveedor de servicios TI. Asimismo, verifica el registro de las incidencias masivas reportadas.	Preventivo	X		El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Manual y debería ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado

Identificación		Identificación			Efectividad		Calificación del Control							
							Diseño				Ejecución		Calificación del Control	Calificación del Grupo de Controles
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización					
R4	Posibilidad de pérdida económica por un inadecuado análisis y diseño de pruebas en control de calidad.	C1	Semanalmente el Comité de Cambios, revisa el impacto al negocio y la arquitectura del sistema, asimismo, el detalle del despliegue en la Gestión de Cambios a TI.	Preventivo	X		El control se encuentra documentado y actualizado.	El control mitiga el riesgo efectivamente	Control Automatizado depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 75% a 89%	5	Moderado	Moderado
		C2	Cada vez que se remita un requerimiento de cambio a TI, el Analista de Control de Calidad, valida que la solución cuente con los documentos requeridos según la metodología vigente y realiza la verificación de la funcionalidad en el ambiente de calidad.	Preventivo	X		El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control combinado (manual-automatizado)	1	Cumplimiento entre 75% a 89%	5	Débil	
		C3	Cada vez que se remita un requerimiento de cambio a TI, el usuario verifica y realiza pruebas en el ambiente de calidad, donde brinda conformidad o emite	Preventivo	X		El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo efectivamente	Control combinado (manual-automatizado)	5	Cumplimiento entre 75% a 89%	5	Moderado	

Identificación		Identificación			Efectividad		Calificación del Control							
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	Diseño				Ejecución		Calificación del Control	Calificación del Grupo de Controles
							A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización					
			observaciones según corresponda.											
R5	Posibilidad de pérdida económica debido a indisponibilidad de los servicios.	C1	En el Comité de Cambios y Pases de Tecnología, se valida el alcance e impacto de cada uno de los pases o cambios presentados para así determinar si es un cambio crítico o no.	Preventivo	X		El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 90% a 100%	10	Fuerte	Fuerte
		C2	Cuando el Comité de Cambios y Pases de Tecnología, determina que el cambio es crítico se solicita un plan de despliegue y las validaciones correspondientes	Preventivo	X		El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 90% a 100%	10	Fuerte	
R6	Posibilidad de pérdida económica por errores en las operaciones	C1	Cada vez que se va a realizar un versionamiento de fuentes, el Analista de Sistemas hace uso de la	Preventivo	X		El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control combinado (manual-automatizado)	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado

Identificación		Identificación			Efectividad		Calificación del Control							
							Diseño				Ejecución		Calificación del Control	Calificación del Grupo de Controles
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización					
	efectuadas en el sistema debido a una administración inadecuada de fuentes.		herramienta informática, donde el Especialista en Software y Aplicaciones custodia y actualiza la fuentes, a fin de usar la última versión disponible.											
		C2	Cada vez que hay un desarrollo, el Jefe de Proyectos de TI revisa si el código fuente entregado, integra todos los cambios paralelos y verifica si este proviene de la versión liberada en línea de la base de producción.	Preventivo	X		El control se encuentra documentado y actualizado.	El control mitiga el riesgo efectivamente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 75% a 89%	5	Moderado	
R7	Posibilidad de pérdida económica por daño y/o pérdida de los backup's de información del banco afectando la disponibilidad e	C1	Cada vez que se produzca una actualización en el inventario, el Jefe de Sección de Infraestructura y Control de Calidad revisa que el proveedor de servicios TI mantenga un inventario	Preventivo	X		El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 75% a 89%	5	Moderado	Moderado

Identificación		Identificación			Efectividad		Calificación del Control							
							Diseño				Ejecución		Calificación del Control	Calificación del Grupo de Controles
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización					
	integridad de la información.		actualizado de los medios magnéticos del Banco que se encuentran en las instalaciones del proveedor de servicios TI.											
		C2	Cada vez que se generen copias de seguridad, el Banco cuenta con 02 cintoteca donde se resguarda la información, las cuales se encuentran en las instalaciones de los proveedores de TDP y Iron Mountain.	Preventivo		X	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 75% a 89%	5	Moderado	
		C3	De acuerdo con el Plan de Pruebas y Mantenimiento Anual de Continuidad del Negocio, el jefe de Sección de Riesgo Operacional y Continuidad del Negocio coordina y	Detectivo		X	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control combinado (manual-automatizado)	5	Cumplimiento entre 75% a 89%	5	Moderado	

Identificación		Identificación			Efectividad		Calificación del Control							
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	Diseño				Ejecución		Calificación del Control	Calificación del Grupo de Controles
							A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización					
			ejecuta 04 pruebas de restauración.											
		C4	Cada vez que se destruirá un medio magnético, el Jefe de Dpto. de Gestión de Servicios de TI verifica la vigencia o mal estado de los medios magnéticos que serán destruidos por el proveedor de Servicios TI.	Preventivo	X		El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	
R8	Posibilidad de pérdida económica por divergencia de responsabilidades de los servicios ofrecidos por el proveedor.	C1	Ante la discrepancia de responsabilidades, son tratados en el Comité de Seguimiento Operativo con el proveedor, donde se llega a un acuerdo o hay un nivel de escalamiento en el Comité Ejecutivo donde se toman decisiones respecto a la responsabilidad.	Detectivo	X		El control no se encuentra documentado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado

Identificación		Identificación			Efectividad		Calificación del Control							
							Diseño				Ejecución		Calificación del Control	Calificación del Grupo de Controles
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización					
		C2	Cada vez que se requiera cambiar un lineamiento del alcance del servicio del contrato, debe pasar por un Control de Cambios con aprobación de ambas partes, antes de su puesta en producción. Es preciso indicar que el costo adicional, solo sería factible posterior a un control de cambios o propuesta adicional de servicio previa aprobación del Banco.	Detectivo	X		El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 75% a 89%	5	Moderado	

Identificación		Identificación			Efectividad		Calificación del Control							
							Diseño				Ejecución			
N° Riesgo	Descripción del Riesgo	Cód	Descripción Del Control	Categoría de Control	Frec	Imp	A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización				Calificación del Control	Calificación del Grupo de Controles
R9	Posibilidad de pérdida económica por la indisponibilidad de servicios TI debido a que no se tiene establecido los horarios de los servicios.	C1	Cada vez que se requiera verificar la disponibilidad de los servicios TI, se tiene establecido el horario de los servicios de los sistemas del SIAF y FITBANK que se brindan en las agencias del banco.	Preventivo	X		El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado
R10	Posibilidad de pérdida económica por no realizar seguimiento a los activos tecnológicos (PC's, Laptops, etc.).	C1	Cada vez que se asigna, da de baja a un activo tecnológico; el Analista de Gestión de Servicios TI tiene la responsabilidad de actualizar el inventario y enviarlo mediante correo electrónico al Jefe de Dpto. de Gestión de Servicios TI.	Preventivo	X		El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado

Nota: La tabla contiene el riesgo identificado con su respectivo control calificado, así como también la calificación individual del diseño y ejecución del control.

Posteriormente a la calificación del grupo de controles, se evaluó el efecto de la calificación del grupo de controles sobre el riesgo inherente para obtener el nivel de riesgo residual (Extremo, Alto, Medio o Bajo). Para ello, se debe considerar lo siguiente:

Tabla 18 *Impacto de la calificación del control sobre el nivel de riesgo*

Calificación Total del Control	Frecuencia	Impacto
Débil	0 niveles hacia abajo	0 niveles hacia abajo
Moderado	1 nivel hacia abajo	1 nivel hacia abajo
Fuerte	2 niveles hacia abajo	2 niveles hacia abajo

Nota: Adaptado del "MPP de Riesgo Operacional", por la entidad financiera. (2020)

La calificación de los riesgos residuales que se obtuvo es la siguiente:

Tabla 19 *Calificación del nivel de riesgo residual*

N° Riesgo	Descripción del Riesgo	Frec	Imp	Nivel Del Riesgo Inherente	Control	Frec	Imp	Calificación del Grupo de Controles	Frec	Imp	Nivel Del Riesgo Residual
R1	Posibilidad de pérdida económica por no identificar de forma correcta a los usuarios en la atención de solicitudes.	4	2	**ALTO**	C1	X		Moderado	3	2	**MEDIO**
					C2	X					
R2	Posibilidad de pérdida económica debido a una inadecuada y/o inoportuna atención de incidentes / requerimientos en los plazos establecidos.	5	1	**ALTO**	C1	X		Moderado	4	1	**MEDIO**
					C2	X					
					C3	X					
					C4	X					

N° Riesgo	Descripción del Riesgo	Frec	Imp	Nivel Del Riesgo Inherente	Control	Frec	Imp	Calificación del Grupo de Controles	Frec	Imp	Nivel Del Riesgo Residual
R3	Posibilidad de pérdida económica debido a no contar con un adecuado control de las solicitudes de requerimientos /incidentes atendidos por el proveedor.	4	3	**ALTO**	C1	X		Moderado	3	3	**ALTO**
R4	Posibilidad de pérdida económica por un inadecuado análisis y diseño de pruebas en control de calidad.	4	1	**MEDIO**	C1	X		Moderado	3	1	**MEDIO**
					C2	X					
					C3	X					
R5	Posibilidad de pérdida económica debido a indisponibilidad de los servicios.	5	1	**ALTO**	C1	X		Fuerte	3	1	**MEDIO**
					C2	X					
R6	Posibilidad de pérdida económica por errores en las operaciones efectuadas en el sistema debido a una administración inadecuada de fuentes.	4	2	**ALTO**	C1	X		Moderado	3	2	**MEDIO**
					C2	X					
R7	Posibilidad de pérdida económica por daño y/o pérdida de los backup's de información del banco afectando la disponibilidad e integridad de la información.	3	4	**EXTREMO**	C1	X		Moderado	2	3	**MEDIO**
					C2		X				
					C3		X				
					C4	X					
R8	Posibilidad de pérdida económica por divergencia de	3	3	**ALTO**	C1	X		Moderado	2	3	**MEDIO**

N° Riesgo	Descripción del Riesgo	Frec	Imp	Nivel Del Riesgo Inherente	Control	Frec	Imp	Calificación del Grupo de Controles	Frec	Imp	Nivel Del Riesgo Residual
	responsabilidades de los servicios ofrecidos por el proveedor.				C2	X					
R9	Posibilidad de pérdida económica por la indisponibilidad de servicios TI debido a que no se tiene establecido los horarios de los servicios.	3	3	**ALTO**	C1	X		Moderado	2	3	**MEDIO**
R10	Posibilidad de pérdida económica por no realizar seguimiento a los activos tecnológicos (PCs, Laptops, etc.).	4	2	**ALTO**	C1	X		Moderado	3	2	**MEDIO**

Nota: La tabla contiene el riesgo identificado con su respectiva calificación de control y el nivel de riesgo residual.

4.3.5. Indicadores clave de riesgos

Los indicadores clave de riesgos, son métricas que permiten tener una señal temprana ante el potencial riesgo. Por ello, se realiza un monitoreo para así determinar la necesidad de implementar medidas correctivas y preventivas con el objetivo de mitigar la posible ocurrencia o materialización de los riesgos.

La necesidad de establecer indicadores clave de riesgos (KRI) es de acuerdo con la calificación obtenida del nivel de riesgo residual.

Tabla 20 *Necesidad de Indicador Clave de Riesgo según nivel de riesgo residual*

Nivel de Riesgo Residual	Necesidad de Indicador Clave de Riesgo (KRI)
Bajo	Opcional
Medio	Opcional
Alto	Obligatorio

Extremo	Obligatorio

Nota: Adaptado del "MPP de Riesgo Operacional", por la entidad financiera. (2020)

Con los colaboradores participantes del taller, se establecieron los siguientes indicadores con el objetivo de monitorear y realizar un seguimiento a los riesgos:

- Porcentaje de requerimientos no atendidos en los plazos planificados por la División de Operación y Tecnología.
- Porcentaje de requerimientos / incidentes clasificados de forma incorrecta
- Número de rechazos debido a errores en la ejecución del pase al ambiente de calidad.
- Número de pases a producción con errores
- Número de copias de respaldo resguardadas
- Número de activos tecnológicos dañados o perdidos

4.3.6. Planes de Acción

Según la calificación obtenida del nivel de riesgo residual se determina la necesidad de establecer planes de acción de acuerdo con el siguiente cuadro:

Tabla 21 *Necesidad de Plan de Acción según nivel de riesgo residual*

Nivel de Riesgo Residual	Necesidad de Plan de Acción (PA)	Plazo de implementación del PA
Bajo	Opcional	----
Medio	Opcional	----
Alto	Obligatorio	9 meses
Extremo	Obligatorio	6 meses

Nota: Adaptado del "MPP de Riesgo Operacional", por la entidad financiera. (2020)

Se coordinó con los participantes del taller y se obtuvo el consenso del equipo de soporte para establecer los siguientes planes de acción con la finalidad de mitigar los riesgos

mencionados. Asimismo, para cada plan de acción se estableció un responsable de implementación y la fecha de compromiso de la implementación del plan de acción.

Tabla 22 *Planes de Acción del proceso de Gestión de Tecnología*

N° Riesgo	Descripción del Riesgo	Nivel Del Riesgo Residual	Código PA	Plan De Acción	Responsable	Plazo
R1	Posibilidad de pérdida económica por no identificar de forma correcta a los usuarios en la atención de solicitudes.	**MEDIO**	PDA001	Formalizar el procedimiento de identificación de usuario final para la atención de solicitud de requerimientos respecto a cambios de contraseña y/o activación de usuario.	Jefe de Dpto. Gestión de Servicios TI	30/06/2020
			PDA002	Evaluar la factibilidad de implementar una herramienta, la cual permita solicitar atención de requerimiento o atender incidencias utilizando las credenciales de red (usuario y contraseña). Asimismo, mediante esta herramienta dar un seguimiento al estado del ticket y el personal responsable.	Jefe de Dpto. Gestión de Servicios TI	30/11/2020
			PDA003	Implementar el IVR (respuesta de voz interactiva) solo para desbloqueo de cuenta y reseteo de contraseña de red previa aprobación de GSTI, SI, tomando en cuenta la validación del DNI y código de empleado y numero de celular.	Jefe de Dpto. Gestión de Servicios TI	31/12/2020
R2	Posibilidad de pérdida económica debido a una inadecuada y/o inoportuna atención de incidentes / requerimientos en los plazos establecidos.	**MEDIO**	PDA002	Evaluar la factibilidad de implementar una herramienta, la cual permita solicitar atención de requerimiento o atender incidencias utilizando las credenciales de red (usuario y contraseña). Asimismo, mediante esta herramienta dar un seguimiento al estado del ticket y el personal responsable.	Jefe de Dpto. Gestión de Servicios TI	30/11/2020
			PDA004	Actualizar la guía de los lineamientos de priorización de tickets.	Jefe de Dpto. Gestión de Servicios TI	30/04/2020
			PDA005	Actualizar la normativa vigente NBD-TS-15 DGG Gestión de Requerimientos de TI con respecto a la gestión actual de	Jefe de Dpto. de Procesos	28/02/2020

N° Riesgo	Descripción del Riesgo	Nivel Del Riesgo Residual	Código PA	Plan De Acción	Responsable	Plazo
				los requerimientos de desarrollo y los documentos necesarios.		
			PDA006	Generar un reporte diario de las incidencias críticas, el cual permita al Dpto. de Gestión de Servicios TI hacer un seguimiento sobre el estado de las atenciones pendientes (Motivo de no atención del ticket, horario de solicitud del ticket y horario de atención planificado)	Analista de Gestión de Servicios TI	31/03/2020
R3	Posibilidad de pérdida económica debido a no contar con un adecuado control de las solicitudes de requerimientos /incidentes atendidos por el proveedor.	**ALTO**	PDA007	Generar un reporte quincenal de los requerimientos e incidencias priorizados, el cual permita al Dpto. de Gestión de Servicios TI hacer una validación de la categoría asignada de priorización es la correcta. Asimismo, este control debe incluirse en la normativa correspondiente.	Analista de Gestión de Servicios TI	30/04/2020
R4	Posibilidad de pérdida económica por un inadecuado análisis y diseño de pruebas en control de calidad.	**MEDIO**	PDA008	Actualizar la normativa vigente NBD-TS-03 DGG Control de Calidad con respecto a los lineamientos, políticas y flujos actuales. Asimismo, especificar que para realizar un pase a producción es necesaria la conformidad y los documentos de pruebas realizados por el usuario.	Jefe de Dpto. de Procesos	31/05/2020
R5	Posibilidad de pérdida económica debido a indisponibilidad de los servicios.	**MEDIO**	PDA009	Actualizar la normativa con el procedimiento correspondiente a la aprobación y evaluación de los pases de emergencia. Así como también quienes conforman un comité de Cambios y pases de Tecnología.	Jefe de Dpto. de Procesos	30/04/2020
			PDA010	Asegurar que las actas del comité de cambios sean entregadas para la validación y firmas correspondientes dentro de los plazos establecidos.	Jefe de Proyectos TI	29/02/2020

Nota: La tabla contiene los planes de acción establecidos con su respectivo responsable y plazo de implementación por cada riesgo identificado.

Capítulo 5: Análisis y Resultados

5.1. Análisis Financiero

En la tabla 23, se precisa el flujo de caja donde se consideró los costos involucrados en la gestión de recursos humanos, gastos de equipos, artículos de oficina y también el promedio de las pérdidas estimadas en base al año 2018-2019. Asimismo, para el cálculo de los ingresos se consideró el monto que se dejó de perder por la mala gestión o indisponibilidad de los servicios de TI.

Tabla 23 *Fujo de Caja del proyecto*

CONCEPTO	Nov-19	Dic-19	Ene-20	Feb-20
EGRESOS	**-44,871.10**	**-44,871.10**	**-44,871.10**	**0.00**
Gestión de Recursos Humanos	17,050.00	17,050.00	17,050.00	-
Gastos de Equipos y Artículos de Oficina	2,000.00	2,000.00	2,000.00	-
Pérdida mensual estimada en base a las pérdidas (Agosto 2018 hasta Julio 2019)	25,821.10	25,821.10	25,821.10	-
INGRESOS	**0.00**	**0.00**	**0.00**	**25,821.10**
Ahorro de la pérdida por mala gestión de TI	0.00	0.00	0.00	25,821.10
FLUJO DE CAJA	**-44,871.10**	**-44,871.10**	**-44,871.10**	**25,821.10**
SALDO ACUMULADO	**-44,871.10**	**-89,742.21**	**-134,613.31**	**-108,792.21**

CONCEPTO	Mar-20	Abr-20	May-20	Jun-20
EGRESOS	**0.00**	**0.00**	**0.00**	**0.00**
Gestión de Recursos Humanos	-	-	-	-
Gastos de Equipos y Artículos de Oficina	-	-	-	-
Pérdida mensual estimada en base a las pérdidas (Agosto 2018 hasta Julio 2019)	-	-	-	-
INGRESOS	**25,821.10**	**25,821.10**	**25,821.10**	**25,821.10**
Ahorro de la pérdida por mala gestión de TI	25,821.10	25,821.10	25,821.10	25,821.10
FLUJO DE CAJA	**25,821.10**	**25,821.10**	**25,821.10**	**25,821.10**
SALDO ACUMULADO	**-82,971.10**	**-57,150.00**	**-31,328.90**	**-5,507.79**

CONCEPTO	Jul-20	Ago-20	Set-20	Oct-20	Nov-20
EGRESOS	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Gestión de Recursos Humanos	-	-	-	-	-
Gastos de Equipos y Artículos de Oficina	-	-	-	-	-
Pérdida mensual estimada en base a las pérdidas (Agosto 2018 hasta Julio 2019)	-	-	-	-	-
INGRESOS	**25,821.10**	**25,821.10**	**25,821.10**	**25,821.10**	**25,822.10**
Ahorro de la pérdida por mala gestión de TI	25,821.10	25,821.10	25,821.10	25,821.10	25,822.10
FLUJO DE CAJA	**25,821.10**	**25,821.10**	**25,821.10**	**25,821.10**	**25,822.10**
SALDO ACUMULADO	**20,313.31**	**46,134.41**	**71,955.52**	**97,776.62**	**123,598.72**

Nota: La tabla contiene el detalle del flujo de caja del proyecto desde el periodo de noviembre 2019 hasta noviembre 2020.

Se procede a realizar el cálculo de los indicadores financieros con la información obtenida del flujo de caja. Para ello, se consideró un costo de oportunidad de capital de 13.02% (ver Anexo 4), debido a que el flujo se toma de un periodo anual se convierte la tasa de descuento a mensual teniendo como resultado de la tasa de descuento a 1.03%.

Como se observa en la tabla 24, se obtiene los indicadores de evaluación donde el valor actual neto (VAN) es de S/ 105,968.55 y la tasa interna de retorno (TIR mensual) de 11.27%. Se concluye que el proyecto es financieramente viable.

Tabla 24 *Indicadores Financieros*

Indicadores Financieros	
VAN	S/105,968.55
TIR	11.27%

Nota: Elaboración propia.

Conclusiones

En el presente documento se ha expuesto la forma de mejorar el proceso de gestión de tecnología aplicando las metodologías de la gestión de riesgo operacional, donde se identificó y analizo todos los riesgos que afectan al proceso, permitiendo a la organización gestionar y priorizar de forma adecuada los riesgos de acuerdo con el nivel de exposición. De esta manera, se adoptaron medidas necesarias, las cuales ayudan a fortalecer los controles y así mitigar o evitar la potencial materialización de los riesgos y que generen pérdidas relacionadas al desarrollo del proceso; por lo cual, la entidad financiera dejo de perder S/25,821.10 mes a mes. Cabe precisar que, la aceptación de un riesgo depende del Apetito y Límite al riesgo operacional que la organización define. También, se estableció indicadores clave de riesgos (KRI's) para el seguimiento y monitoreo del desempeño de los riesgos con mayor nivel asociado al proceso.

Para el desarrollo del informe se utilizó las metodologías de autoevaluación de riesgos y controles, indicadores clave de riesgos y planes de acción con la finalidad de conocer en profundidad el proceso de una adecuada gestión de riesgos operacionales en los procesos de la organización. Si bien es cierto, la administración adecuada de los riesgos operacionales no aporta en el crecimiento de las ventas, pero contribuye a la organización respecto a la reducción de los gastos por pérdidas relacionadas al riesgo operacional que están asociadas a los procesos, por ende, la rentabilidad aumentaría.

En el proceso de Gestión de Tecnología se identificaron y analizaron 10 riesgos operacionales según el valor de impacto y frecuencia, donde se obtuvo como resultado que uno tiene el nivel de riesgo residual Alto y nueve tienen el nivel de riesgo residual Medio. Cabe precisar que cada riesgo cuenta con sus respectivas causas y consecuencias.

Por otro lado, en el proceso en mención se detectó que existen 22 controles que se encuentran asociados a los riesgos operacionales y se realizó la evaluación de estos en base al

diseño y la ejecución del control, donde se obtuvo como resultado que la mayoría (18) de controles tienen una calificación moderada, un control débil y tres controles con calificación fuerte.

Asimismo, se establecieron 06 indicadores clave de riesgos con sus umbrales correspondientes a cargo de la División de Operaciones y Tecnología, quienes deberán reportar según la frecuencia al Departamento de Riesgo de Operación con la finalidad de realizar un seguimiento y monitoreo que nos permita tener un sistema de alerta temprana del deterioro del perfil de riesgo.

Finalmente, se establecieron 10 planes de acción a cargo del Departamento de Gestión de Servicios TI y del Departamento de Procesos, los cuales tenían como fecha de implementación para el año 2020, con el objetivo de mitigar la ocurrencia de los riesgos detectados en el proceso.

Recomendaciones

- Se recomienda incluir en el plan de trabajo de la Gestión de Riesgo Operacional realizar la revisión de los demás procesos principales y secundarios con la finalidad de mejorar los procesos de la entidad financiera.
- Se recomienda realizar capacitaciones y/o entrenamiento a los gestores, coordinadores de riesgos y personal administrativo respecto a las metodologías de riesgo operacional (autoevaluación de riesgos y controles, indicadores clave de riesgos y planes de acción), con la finalidad de que los responsables del proceso tengan la capacidad de identificar y sus propios riesgos.
- Se recomienda a la gerencia de TI realizar reuniones de trabajo con el equipo responsable de los planes de acción para afianzar el compromiso del cumplimiento de los planes de acción con la finalidad de mitigar la exposición de los riesgos del proceso.
- Se recomienda realizar un testeo de los controles del proceso de Gestión de Tecnología con la finalidad de garantizar que estos están siendo aplicados de forma correcta y verificar la efectividad de los controles.
- Realizar el seguimiento al cumplimiento de la implementación de los planes de acción mencionados en el presente Trabajo de Suficiencia Profesional, así como también la reportería de los indicadores con el objetivo de mejorar los controles del proceso y llevar un monitoreo adecuado de los indicadores clave de riesgos.

Referencias

ACL. (2017,13 de Febrero). *¿Qué es el desarrollo de SW?*. https://www.acl.cl/que-es-el-desarrollo-de-software/

Alexander, A., Anduig, M., Arcenegui, J., Arranz, J., Carrillo, S., Corcóstegui, C., & Costero, R., et al. (2010) *La gestión del riesgo operacional: de la teoría a su aplicación* (1ª.ed.). México, D.F: Limusa.

Asociación de Administradoras Fondos Mutuos Perú. (2020). *Informe de Fondos Mutuos Diciembre 2020*. https://fondosmutuos.pe/wp-content/uploads/2021/02/Informe-Diciembre-2020.pdf

Aprueban Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos y establecen otras disposiciones (2017). Recuperado de: https://busquedas.elperuano.pe/normaslegales/aprueban-reglamento-de-gobierno-corporativo-y-de-la-gestion-resolucion-no-272-2017-1476592-1/

Banco de Comercio. (2019). *Memoria Anual 2019*. https://www.bancomercio.com/repositorioaps/0/0/jer/memoria_anual/files/Memoria%20Anual%202019.pdf

Banco de Comercio. (2021). *Misión, Visión y Valores*. https://www.bancomercio.com/elbanco/categoria/mision-vision-y-valores/10/c-10

Gil, V., & Gil, J. (2017). *Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas*. Recuperado de: https://www.redalyc.org/pdf/849/84953103011.pdf

Hanna, A. & Rance, S. (2011). Glosario y abreviatura de ITIL. Recuperado de: http://www.itil-officialsite.com/InternationalActivities/TranslatedGlossaries.aspx

Instituto Nacional de Estadística e Informática (2010). *Clasificación Industrial Internacional Uniforme Revisión 4*. https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib0883/Libro.pdf

ISOTools Excellence (2020). *Norma ISO 31000: el valor de la gestión de riesgos en las organizaciones*. https://www.isotools.org/pdfs-pro/ebook-iso-31000-gestion-riesgos-

organizaciones.pdf?utm_campaign=ISO%2031000&utm_medium=email&_hsmi=25816197&_hsenc=p2ANqtz-86PgB2mNpKP-afYL8qThqofr3ecJrC-mhXupuDXb98gwGHGtLgJlVIORTiQv_SHekkGG3WC0ARpq_E_XC8XsIPNMp7hA&utm_content=25816197&utm_source=hs_automation

ITIL. (2011). *Glosario y abreviaturas de ITIL*. http://www.itil-officialsite.com/InternationalActivities/TranslatedGlossaries.aspx

Jaimes, M., Ramírez, D., Vargas, A., & Carrillo, G. (2011). Gestión Tecnológica: conceptos y casos de aplicación. *Gerencia Tecnología Información, 10, 43-54*.

Kempter, S. (2016). *ITIL Gestión de Cambios*. https://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_Cambios

ManageEngine Service Desk Plus. (2020). *Guía de gestión de cambios*. https://www.manageengine.com/latam/service-desk/itsm/que-es-la-gestion-de-cambios.html

Ministerio de Economía y Finanzas. (2020). *El Poder Ejecutivo promulgó hoy la Ley que modifica diversas leyes para facilitar la inversión, impulsar el desarrollo productivo y el crecimiento empresarial*. https://www.mef.gob.pe/es/?id=3262%&I=&option=com_content&language=es-ES&view=article&lang=es-ES

Ministerio de Hacienda y Administraciones Públicas (2012). *Metodología de Análisis y gestión de Riesgos de los Sistemas de Información (Versión 3).* Madrid: Portal de Administración Electrónica.

Pacific Credit Rating. (2018). *Clasificación del Banco de Comercio*. https://www.ratingspcr.com/application/files/6715/4091/9181/Banco_de_Comercio01.pdf#:~:text=El%20Banco%20de%20Comercio%20est%C3%A1,ser%20el%20Banco%20de%20la

Pacific Credit Rating. (2020). *Clasificación del Banco de Comercio*. https://www.ratingspcr.com/application/files/2816/0191/2274/PE-BCO-202006-FIN-FFDCPDMPDLPBS.pdf

Pérez, J. (2004). *Gestión por procesos. Cómo utilizar ISO 9001:2000 para mejorar la gestión de la organización*. https://gestiondecalidadmpn.files.wordpress.com/2012/02/01-

pc3a9rez-gestic3b3n-por-procesos-cc3b3mo-utilizar-iso-9001-2000-para-mejorar-la-gestic3b3n-de-la-organiz.pdf

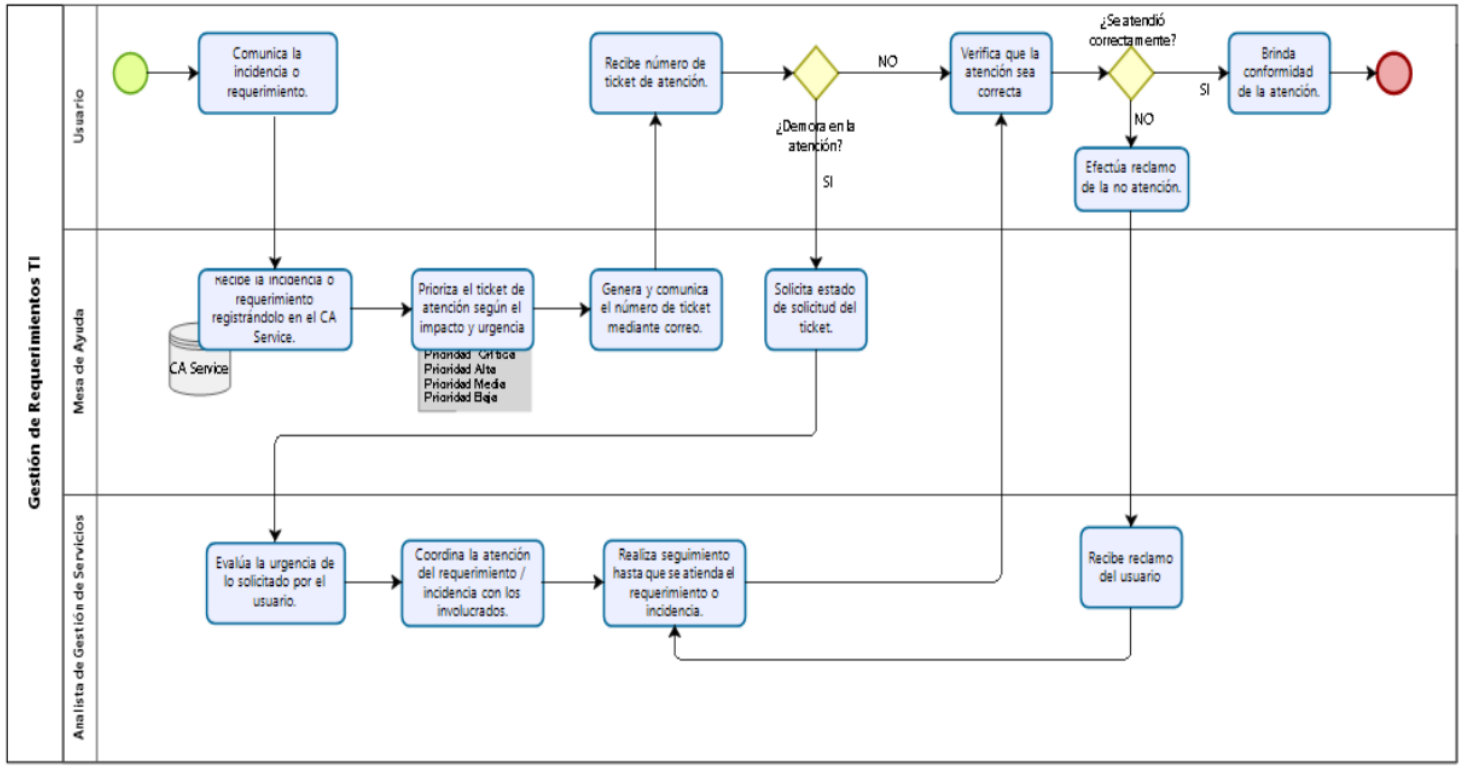
Superintendencia de Banca, Seguros y AFP. (s.f.). ¿Qué es la SBS? Recuperado de: https://www.sbs.gob.pe/acercadelasbs

Superintendencia de Banca, Seguros y AFP (2009). *Reglamento para la Gestión del Riesgo Operacional*. Repositorio intranet SBS https://intranet2.sbs.gob.pe/dv_int_cn/842/v1.0/Adjuntos/2116-2009.r.pdf

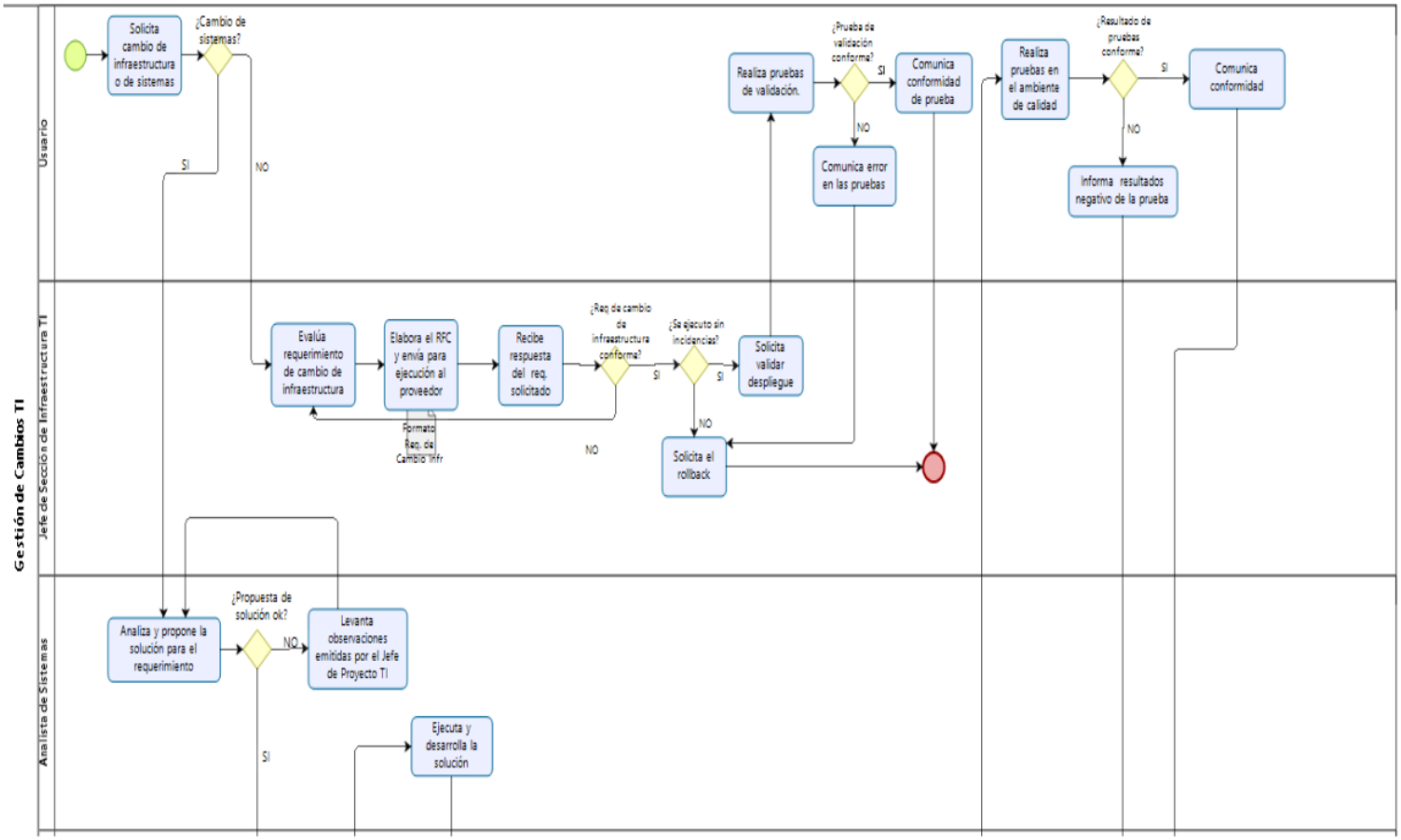
Superintendencia de Banca, Seguros y AFP (2017). *Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos*. Repositorio intranet SBS https://intranet2.sbs.gob.pe/dv_int_cn/1708/v3.0/Adjuntos/272-2017.R.pdf

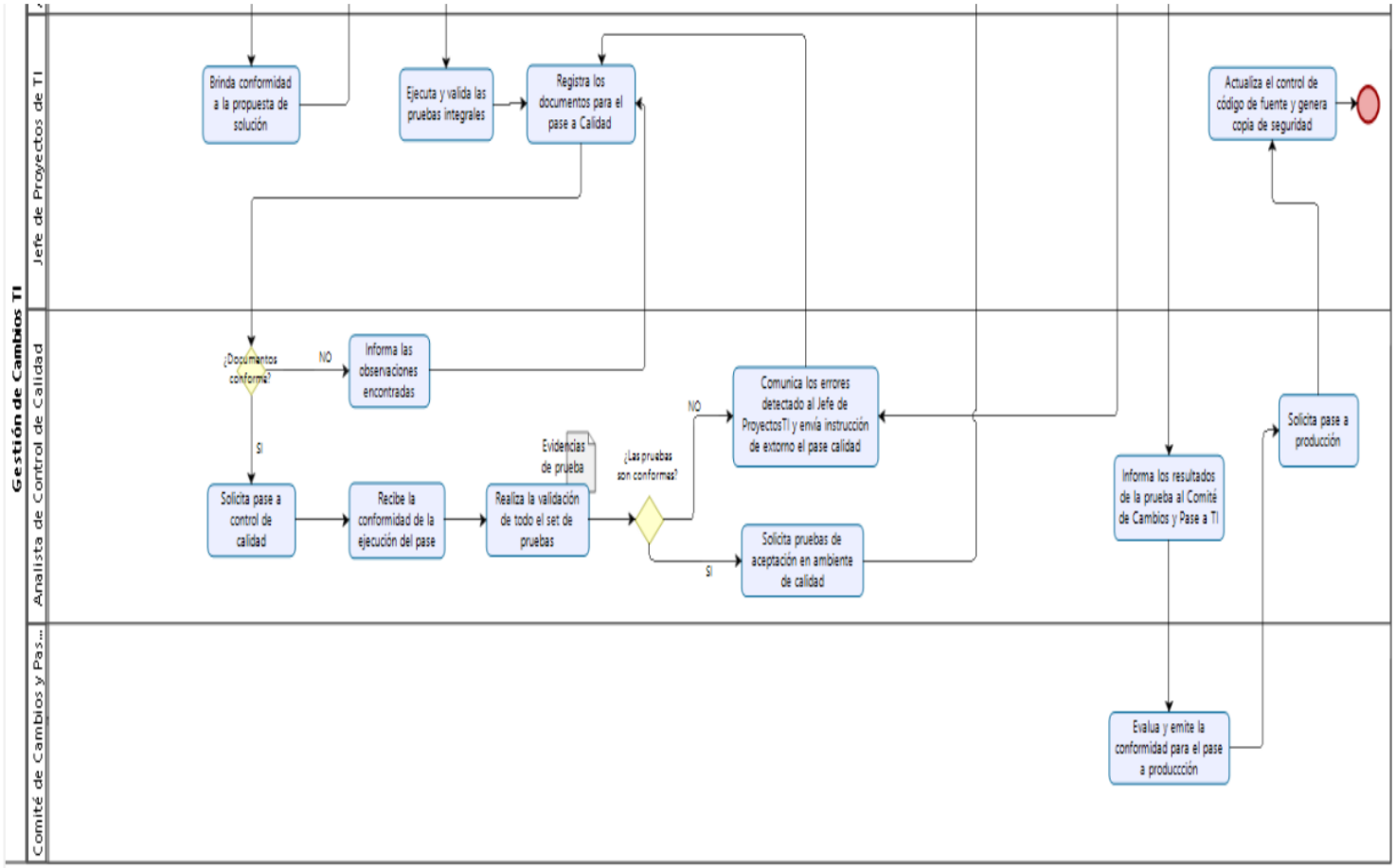
Anexos

Anexo 1 - Diagrama de Flujo del Proceso de Gestión de Requerimientos TI



Anexo 2 - Diagrama de Flujo del Proceso de Gestión de Cambios TI




Gestión de Cambios TI
Jefe de Proyectos de TI
Analista de Control de Calidad
Comité de Cambios y Pas...
Brinda conformidad a la propuesta de solución
Ejecuta y valida las pruebas integrales
Registra los documentos para el pase a Calidad
Actualiza el control de código de fuente y genera copia de seguridad
¿Documentos conforme?
NO
Informa las observaciones encontradas
SI
Solicita pase a control de calidad
Recibe la conformidad de la ejecución del pase
Realiza la validación de todo el set de pruebas
Evidencias de prueba
¿Las pruebas son conformes?
NO
Comunica los errores detectado al Jefe de ProyectosTI y envía instrucción de extorno el pase calidad
SI
Solicita pruebas de aceptación en ambiente de calidad
Informa los resultados de la prueba al Comité de Cambios y Pase a TI
Solicita pase a producción
Evalua y emite la conformidad para el pase a producción

Anexo 3 – Matriz de Riesgos y Controles de Gestión de Tecnología

Identificación							Identificación			Efectividad		Definición				Calificación del Control							Evaluación Riesgo Residual		
																Diseño									
N° Riesgo	Proceso	Sub-proceso	Descripción del Riesgo	Causas	Consecuencias	Nivel Del Riesgo Inherente	Control	Descripción Del Control	Categoria de Control	Frecuencia	Impacto	1. Responsable	2. Frecuencia	3. Deja Evidencias electrónica o física?	4. Está Normado o documentado?	A. Nivel de Definición	B. Cumple su objetivo?	C. Nivel de Automatización		Ejecución		Calificación del Control	Calificación del Grupo de Controles	Frecuencia	Impacto	Nivel Del Riesgo Residual
R1	Gestión de Tecnología	Gestión de Requerimientos TI	Posibilidad de pérdida económica por no identificar de forma correcta a los usuarios en la atención de solicitudes.	1. Falta de mecanismos para la identificación de usuario final por parte de Mesa de Ayuda.	1.Suplantación de identidad (Fraude Interno) 2.Fuga de Información	ALTO	C1	Cada vez que se solicite la atención de una solicitud, el personal de Mesa de Ayuda solicita codigo de empleador o DNI del usuario final para verificar la autenticación.	Preventivo	X		Mesa de Ayuda	Cada vez que se ejecuta	NO	NO	El control no se encuentra documentado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado	3	2	MEDIO
							C2	Se ha habilitado a los Gerentes de Agencias la opción de desbloqueo de cuentas de los colaboradores de sus equipos, estos usuarios no requieren llamar a Mesa de Ayuda.	Preventivo	X		Gerente de Agencia	Cada vez que se ejecuta	SI	NO	El control no se encuentra documentado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado				
R2	Gestión de Tecnología	Gestión de Requerimientos TI	Posibilidad de pérdida económica debido a una inadecuada y/o inoportuna atención de incidentes / requerimientos en los plazos establecidos.	1. Inadecuada priorización y análisis de la atención de los tickets. 2. Falta de conocimiento de los procesos y sistemas involucrados. 3. Recepción de documentación incompleta y/o incorrecta. 4. Inadecuada elaboración del documento solución. 5. Falta de seguimiento en la atención de incidencias y requerimientos.	1.Reprogramaciones de requerimientos. 2.Multas y/o sanciones del ente regulador. 3.Acumulación de solicitudes 4.Incremento del costo del requerimiento.	ALTO	C1	Cada vez que el usuario realiza una solicitud (requerimiento o incidente), el personal de Mesa de Ayuda anota y realiza la priorización del ticket en base al impacto y urgencia (Prioridad crítica, Alta, Media y Baja) cumpliendo con los tiempo establecidos según la normativa	Preventivo	X		Mesa de Ayuda	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado	4	1	MEDIO
							C2	De forma trimestral, se realiza la capacitación al personal de Mesa de Ayuda respecto a la priorización de los requerimientos y los documentos o sustentos que se debe solicitar según corresponda.	Preventivo	X		Mesa de Ayuda	Trimestral	SI		El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 90% a 100%	10	Fuerte				
							C3	El Analista de Sistemas evalúa el alcance, tiempo, recursos y así determina la solución y atención del requerimiento de TI, en este último caso es coordinado con el Jefe de Proyectos de Tipara su atención.	Preventivo	X		Analista de Sistemas / Jefe de Proyectos TI	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado				
							C4	Cada vez que la atención de un ticket se demora o retrasa, el usuario coordina con el Analista de Gestión de Servicios para el seguimiento de la atención al requerimiento o incidencia	Detectivo	X		Analista de Gestión de Servicios TI	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Manual y debería ser auto matizado	5	Cumplimiento entre 75% a 89%	5	Moderado				
R3	Gestión de Tecnología	Gestión de Requerimientos TI	Posibilidad de pérdida económica debido a no contar con un adecuado control de las solicitudes de requerimiento e incidentes atendidos por el proveedor.	1. Inadecuado registro de solicitudes de requerimiento e incidentes (incidentes independiente o siendo incidencias masivas). 2. Inadecuado control manual o	1. Exceso de costo en el servicio del proveedor de TI.	ALTO	C1	De forma semanal el Opto. de Gestión de Servicio TI realiza las incidencias y requerimiento a fin de controlar el pago de la factura mensual proporcionada por el proveedor de servicios TI. Asimismo, verifica el registro de las incidencias masivas reportadas.	Preventivo	X		Analista de Gestión de Servicios TI	Semanal	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Manual y debería ser auto matizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado	3	3	ALTO
R4	Gestión de Tecnología	Gestión de Cambios de TI	Posibilidad de pérdida económica por un inadecuado análisis y diseño de pruebas en control de calidad.	1. Falta de personal capacitado 2. Pruebas de calidad insuficientes.	1. Cambios puestos en producción con errores o no son los esperados por el usuario. 2.Retrabajo al realizar nuevamente el desarrollo del software. 3.Incumplimiento de plazos	MEDIO	C1	Semanalmente el Comité de Cambios, revisa el impacto al negocio y la arquitectura del sistema, asimismo, el detalle del despliegue en la Gestión de Cambios a TI.	Preventivo	X		Comité de cambios.	Semanal	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo efectivamente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 90% a 100%	10	Fuerte	Moderado	3	1	MEDIO
							C2	Cada vez que se remita un requerimiento de cambio a TI, el Analista de Control de Calidad, valida que la solución cuente con los documentos requeridos según la metodología vigente y realiza la verificación de la funcionalidad en el ambiente de calidad.	Preventivo	X		Analista de Control de Calidad	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control combinado (manual automatizado)	1	Cumplimiento entre 75% a 89%	5	Débil				
							C3	Cada vez que se remita un requerimiento de cambio a TI, el usuario verifica y realiza pruebas en el ambiente de calidad, donde brinda conformidad o emite observaciones según corresponda.	Preventivo	X		Usuario	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo efectivamente	Control combinado (manual automatizado)	5	Cumplimiento entre 75% a 89%	5	Moderado				
R5	Gestión de Tecnología	Gestión de Cambios de TI	Posibilidad de pérdida económica debido a indisponibilidad de los servicios.	1. Inadecuado procedimiento para realizar y dimensionar el impacto de los pases a realizar. 2. Falta de personal técnico para priorizar los cambios requeridos. 3. Error humano 4. No cumplimiento de las	1.Multa del ente regulador por incumplimiento de normativa vigente. 2.Multa del ente regulador debido a	ALTO	C1	En el Comité de Cambios y Pases de Tecnología, se valida el alcance e impacto de cada uno de los pases o cambio presentado para así determinar si es un cambio crítico o no.	Preventivo	X		Comité de Cambios y Pases de Tecnología.	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 90% a 100%	10	Fuerte	Fuerte	3	1	MEDIO
							C2	Cuando el Comité de Cambios y Pases de Tecnología, determina que el cambio es crítico se solicita un ban de despliegue y las validaciones correspondientes	Preventivo	X		Comité de Cambios y Pases de Tecnología.	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 90% a 100%	10	Fuerte				
R6	Gestión de Tecnología	Gestión de Cambios de TI	Posibilidad de pérdida económica por errores en las operaciones efectuadas en el sistema debido a una administración inadecuada de fuentes.	1. Inadecuado versionamiento del código fuente. 2. Problemas en la administración de repositorio de custodia de fuentes. 3. Falta de personal técnico.	1.Multa del ente regulador por evidenciar los clientes. 2.Reparación de incidencias /Comportamiento anómalo del aplicativo. 3.Indisponibilidad de los servicios para la	ALTO	C1	Cada vez que se va realizar un versionamiento de fuentes, el Analista de Sistemas hace uso de la herramienta informática, donde el Especialista en Software y Aplicaciones custodia y actualiza la fuentes, a fin de usar la última versión disponible.	Preventivo	X		Analista de Sistemas	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control combinado (manual automatizado)	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado	3	2	MEDIO
							C2	Cada vez que haya un desarrollo, el Jefe de Proyectos de TI revisa si el código fuente entregado, integra todos los cambios paralelos y verifica si este proviene de la versión liberada en línea de la base de producción.	Preventivo	X		Jefe de Proyectos de TI	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo efectivamente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 90% a 100%	10	Fuerte				
R7	Gestión de Tecnología	Gestión de Servicios TI	Posibilidad de pérdida económica por daño y/o pérdida de los backup's de información del banco afectando la disponibilidad e integridad de la información.	1. Deterioro de los medios magnéticos. 2. Falta de verificación por parte de las áreas de control ante el borrado y destrucción de los medios de almacenamiento (no custodia en que la información ya este almacenada en otro backup, que la información pueda ser omitida) 3. Falta de revisión y verificación de los inventarios de control de medios magnéticos.	1. Multas y/o sanciones 2.Pérdida de información. 3.Riesgo reputacional	EXTREMO	C1	Cada vez que se produzca una actualización en el inventario, el Jefe de Sección de Infraestructura y Control de Calidad revisa que el proveedor de servicios TI mantenga un inventario actualizado de los medios magnéticos del Banco que se encuentran en las instalaciones del proveedor de servicios TI.	Preventivo	X		Jefe de Sección de Infraestructura y Control de Calidad	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 90% a 100%	10	Fuerte	Moderado	2	3	MEDIO
							C2	Cada vez que se generen copias de seguridad, el Banco cuenta con 03 cintoteca donde se resguarda la información, las cuales se encuentran en las instalaciones de los proveedores de TDP y Iron Mountain	Preventivo		X	Jefe de Opto. de Gestión de Servicios de TI	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 75% a 89%	5	Moderado				
							C3	De acuerdo al Plan de Pruebas y Mantenimiento Anual de Continuidad del Negocio, el Jefe de Sección de Riesgo Operacional y Continuidad del Negocio coordina y ejecuta 04 pruebas de restauración (03 de manera independiente y 01 prueba integral).	Detectivo		X	Jefe de Sección de Riesgo Operacional y Continuidad del Negocio	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control combinado (manual automatizado)	5	Cumplimiento entre 75% a 89%	5	Moderado				
							C4	Cada vez que se destruirá un medio magnético, el Jefe de Opto. de Gestión de Servicios de TI verifica la vigencia o real estado de los medios magnéticos que serán destruidos por el proveedor de Servicios TI.	Preventivo	X		Jefe de Opto. de Gestión de Servicios de TI	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado				
R8	Gestión de Tecnología	Gestión de Servicios TI	Posibilidad de pérdida económica por divergencia de responsabilidades de los servicios ofrecidos por el proveedor.	1.Desconocimiento del alcance del contrato. 2.Discrepancias en las responsabilidades por parte del proveedor y del banco.	1.Falta de ejecución de actividades	ALTO	C1	Ante la discrepancia de responsabilidades, son listado a nivel Comité de Seguimiento Operativo con el proveedor, en estas reuniones se llega a un acuerdo o hay un nivel de escalamiento en el Comité Ejecutivo donde se toman decisiones respecto a la responsabilidad.	Detectivo	X		Comité Ejecutivo	Cada vez que se ejecuta	SI	SI	El control no se encuentra documentado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado	2	3	MEDIO
							C2	Cada vez que se requiera cambiar algún lineamiento del alcance del servicio que se considera en el contrato, debe pasar por un Control de Cambio en el Contrato con aprobación de ambas partes, antes de su puesta en producción. Es preciso indicar que el costo adicional, solo sería factible poderlo valorar a un control de cambios o propuesta adicional de servicio previa aprobación del Banco.	Detectivo	X		Representantes del Banco	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado y actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	10	Cumplimiento entre 75% a 89%	5	Moderado				
R9	Gestión de Tecnología	Gestión de Servicios TI	Posibilidad de pérdida económica por la indisponibilidad de servicios TI debido a que no se tiene establecido los horarios de los servicios.	1. No se tiene actualizado los horarios de los servicios TI cada comité en donde se ratifica y se debe incluir todos los servicios incluidos los 24/7). 2. No se tiene establecido los	1. Indisponibilidad de servicios TI 2.Multa y/o sanciones 3.Reclamo de Clientes	ALTO	C1	Cada vez que se requiera verificar la disponibilidad de los servicios TI, se tiene establecido el horario de los servicios de los sistemas del ISAP y FITBANK que se brinda en las agencias del banco.	Preventivo	X		Jefe de Opto. de Gestión de Servicios de TI	Cada vez que se ejecuta	SI	SI	El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado	2	3	MEDIO
R10	Gestión de Tecnología	Gestión de Servicios TI	Posibilidad de pérdida económica por no realizar seguimiento a los activos tecnológicos (PC's, Laptops, etc.).	1. Inadecuado seguimiento y/o supervisión de los activos tecnológicos. 2. Inventario de activos tecnológicos desactualizado. 3. No se encuentra actualizado el	1. Costo de reposición de activos tecnológicos. 2.Pérdida los activos tecnológicos	ALTO	C1	Cada vez que se asigna, da de bajas un activo tecnológico; el Analista de Gestion de Servicios TI tiene la responsabilidad de actualizar el inventario y enviarlo mediante correo electrónico al Jefe de Opto. de Gestión de Servicios TI.	Preventivo	X		Analista de Gestión de Servicios TI	Cada vez que se ejecuta	SI	NO	El control se encuentra documentado, pero no actualizado.	El control mitiga el riesgo parcialmente	Control Automatizado o depende de TI / Control Manual y no es posible ser automatizado	5	Cumplimiento entre 75% a 89%	5	Moderado	Moderado	3	2	MEDIO

Anexo 4 - Tasa de descuento de los fondos mutuos

Descripción de Fondo	SAFM	Rentabilidad 2020 (%)
BBVA Soles	BBVA Asset Management	3.53%
BBVA Soles Monetario	BBVA Asset Management	2.49%
BBVA Perú Soles	BBVA Asset Management	2.07%
Credicorp Capital Conservador Liquidez Soles	Credicorp Capital	1.38%
Credicorp Capital Conservador Mediano Plazo Soles	Credicorp Capital	4.74%
Credicorp Capital Conservador Corto Plazo Soles	Credicorp Capital	3.12%
Diviso Extra Conservador Soles	Diviso Fondos	2.21%
Fondo de Fondos Sura Capital Estratégico I FMIV - Serie A	Fondos Sura	11.47%
Fondo de Fondos Sura Capital Estratégico I FMIV - Serie B	Fondos Sura	11.74%
Fondo de Fondos Sura Capital Estratégico II FMIV - Serie A	Fondos Sura	12.75%
Fondo de Fondos Sura Capital Estratégico II FMIV - Serie B	Fondos Sura	13.02%
Sura Corto Plazo Soles FMIV	Fondos Sura	3.01%
Sura Renta Soles FMIV	Fondos Sura	5.02%
IF Mediano Plazo Soles	Interfondos	2.88%
IF Oportunidad Soles - Serie A	Interfondos	2.18%
IF Oportunidad Soles - Serie B	Interfondos	2.20%
IF Libre Disponibilidad - Serie A	Interfondos	0.96%
IF Libre Disponibilidad - Serie B	Interfondos	1.00%
Promedio de los fondos		**4.77%**

Tesis TSP Gutierrez Mateo Margiori

INFORME DE ORIGINALIDAD

3%	3%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	creativecommons.org Fuente de Internet	1%
2	www.bancomercio.com Fuente de Internet	1%
3	repositorio.unsa.edu.pe Fuente de Internet	1%
4	Submitted to Pontificia Universidad Catolica del Peru Trabajo del estudiante	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		